Documentation

HiPath 8000
OpenStage 20, OpenStage 40, OpenStage 60, OpenStage 80

Administration Manual

A31003-O1010-M100-10-76A9

Communication for the open minded

Siemens Enterprise Communications
www.siemens.com/open

SIEMENS

Content

1 Overview 1-1
1.1 Important Notes 1-1
1.2 Maintenance Notes 1-2
1.3 Product Identification 1-2
1.4 About the Manual 1-2
1.5 Conventions for this Document 1-2
1.6 The OpenStage Family 1-3
1.6.1 OpenStage 60/80 1-3
1.6.2 OpenStage 40 1-4
1.6.3 OpenStage 20 1-6
1.7 Administration Interfaces 1-6
1.7.1 Web-based Management (WBM) 1-6
1.7.2 DLS Service (Deployment Service) 1-7
1.7.3 Local Phone Menu 1-7

2 Startup 2-1
2.1 Prerequisites 2-1
2.2 Assembling and Installing the Phone 2-2
2.2.1 Shipment 2-2
2.2.2 Connectors at the bottom side 2-2
2.2.3 Assembly 2-4
2.2.4 Connecting the Phone 2-5
2.3 Quick Start 2-7
2.3.1 Access the Web Interface (WBM) 2-7
2.3.2 Set the Terminal Number 2-8
2.3.3 Basic Network Configuration 2-10
2.3.4 Date and Time / SNTP 2-10
2.3.5 SIP Server Address 2-10
2.3.6 Extended Network Configuration 2-11
2.3.7 Vendor specific: VLAN Discovery and DLS address 2-11
2.3.7.1 Using a Vendor Class 2-12
2.3.7.2 Using Option #43 "Vendor Specific" 2-20
2.3.8 Registering at the HiPath 8000 2-25

3 Administration 3-1
3.1 Access via Local Phone 3-1
3.2 LAN Settings 3-5
3.2.1 LAN Port Settings 3-5
3.2.2 VLAN 3-7
3.2.2.1 Automatic VLAN discovery (DHCP) 3-8
3.2.2.2 Manual configuration of a VLAN ID 3-9

3.3 IP Network Parameters . . . 3-10
3.3.1 Quality of Service (QoS) . . . 3-10
3.3.1.1 Layer 2 / 802.1p . . . 3-10
3.3.1.2 Layer 3 / Diffserv . . . 3-11
3.3.2 Use DHCP . . . 3-13
3.3.3 IP Address - Manual Configuration . . . 3-15
3.3.4 Default Route/Gateway . . . 3-16
3.3.5 Specific IP Routing . . . 3-17
3.3.6 DNS . . . 3-18
3.3.6.1 DNS Domain Name . . . 3-18
3.3.6.2 DNS Servers . . . 3-19
3.3.7 Configuration & Update Service (DLS) . . . 3-20
3.3.8 SNMP . . . 3-21
3.4 Speech Encryption (V1R4.x upwards) . . . 3-24
3.5 System Settings . . . 3-25
3.5.1 Terminal and User Identity . . . 3-25
3.5.1.1 Terminal Identity . . . 3-25
3.5.1.2 Display Identity . . . 3-26
3.5.2 Emergency and Voice Mail . . . 3-27
3.5.3 Pixel Saver (OpenStage 40/60/80) . . . 3-29
3.5.4 Date and Time . . . 3-30
3.5.4.1 SNTP is available, but no automatic configuration by DHCP server . . . 3-30
3.5.4.2 No SNTP server available . . . 3-32
3.5.5 SIP Addresses and Ports . . . 3-33
3.5.5.1 SIP Addresses . . . 3-33
3.5.5.2 SIP Ports . . . 3-34
3.5.6 SIP Registration . . . 3-35
3.5.7 SIP Connection and Communication . . . 3-37
3.5.7.1 Response Timer . . . 3-37
3.5.7.2 Connectivity Check . . . 3-37
3.5.7.3 Outbound Proxy . . . 3-38
3.5.7.4 SIP Transport Protocol . . . 3-39
3.5.8 SIP Session Timer . . . 3-40
3.5.9 SIP Survivability . . . 3-42
3.6 Features - Configuration . . . 3-45
3.6.1 Allow Refuse . . . 3-45
3.6.2 Group Pickup . . . 3-47
3.6.2.1 Feature Code . . . 3-47
3.6.2.2 Pickup alert (V1R3.x upwards) . . . 3-48
3.6.3 Call Transfer . . . 3-50
3.6.3.1 Transfer on Ring . . . 3-50
3.6.3.2 Transfer on Hangup . . . 3-50
3.6.4 Callback URIs . . . 3-52
3.6.5 Message Waiting Address . . . 3-53

3.6.6 System Based Conference 3-54
3.6.7 Server Based Features (V1R3.x upwards) 3-55
3.6.8 uaCSTA Interface 3-56
3.6.9 Local Menu Timeout 3-58
3.7 Multiline Appearance/Keyset 3-60
3.7.1 Line key configuration 3-60
3.7.2 Configure Keyset Operation 3-64
3.7.3 Direct Station Select (DSS) 3-68
3.7.3.1 General DSS Settings 3-68
3.7.3.2 Settings for a DSS key 3-69
3.7.4 Key Modules 3-71
3.8 Dialing 3-72
3.8.1 Canonical Dialing Configuration 3-72
3.8.2 Canonical Dial Lookup 3-76
3.9 Mobility 3-78
3.10 Transferring Phone Software, Application and Media Files 3-79
3.10.1 FTP/HTTPS Server 3-79
3.10.2 Common FTP/HTTPS Settings 3-79
3.10.3 Phone Software 3-81
3.10.3.1 FTP/HTTPS Access Data 3-81
3.10.3.2 Download/Update Phone Software 3-83
3.10.4 Music on Hold 3-84
3.10.4.1 FTP/HTTPS Access Data 3-84
3.10.4.2 Download Music on Hold 3-87
3.10.5 Picture Clips 3-88
3.10.5.1 FTP/HTTPS Access Data 3-88
3.10.5.2 Download Picture Clip 3-90
3.10.6 LDAP Template 3-91
3.10.6.1 FTP/HTTPS Access Data 3-91
3.10.6.2 Download LDAP Template 3-93
3.10.7 Logo 3-94
3.10.7.1 FTP/HTTPS Access Data 3-94
3.10.7.2 Download Logo 3-96
3.10.8 Screensaver 3-97
3.10.8.1 FTP/HTTPS Access Data 3-97
3.10.8.2 Download Screensaver 3-99
3.10.9 Ringer File 3-100
3.10.9.1 FTP/HTTPS Access Data 3-100
3.10.9.2 Download Ringer File 3-103
3.11 Corporate Phonebook: Directory Settings 3-104
3.11.1 LDAP 3-104
3.12 Speech 3-106
3.12.1 RTP Base Port 3-106
3.12.2 Codec Preferences 3-107

3.12.3 Audio Settings 3-109
3.13 Applications 3-110
3.13.1 XML Applications (OpenStage 60/80 with V1R3.x upwards) 3-110
3.13.1.1 Basic Setup/Configuration 3-110
3.13.1.2 HTTP Proxy 3-113
3.13.1.3 Modify an Existing Application 3-115
3.13.1.4 Remove an Existing Application 3-116
3.14 Password 3-118
3.15 Troubleshooting: Lost Password 3-119
3.16 Factory Reset 3-120
3.17 Diagnostics 3-121
3.17.1 Display General Phone Information 3-121
3.17.2 LAN Monitoring 3-122
3.17.3 IP Tests 3-123
3.17.4 Process and Memory Information 3-124
3.17.5 Fault Trace Configuration 3-125
3.17.6 Easy Trace Profiles 3-131
3.17.6.1 Bluetooth Handsfree 3-131
3.17.6.2 Bluetooth Headset 3-131
3.17.6.3 Call Connection 3-132
3.17.6.4 Call Log 3-132
3.17.6.5 LDAP Phonebook 3-133
3.17.6.6 DAS Connection 3-133
3.17.6.7 DLS Data Errors 3-133
3.17.6.8 802.1x 3-134
3.17.6.9 Help Application 3-134
3.17.6.10 Sidecar 3-134
3.17.6.11 Key Input 3-135
3.17.6.12 LAN Connectivity 3-135
3.17.6.13 Local Phonebook 3-135
3.17.6.14 Messaging 3-136
3.17.6.15 Mobility 3-136
3.17.6.16 Phone administration 3-136
3.17.6.17 Server based applications 3-137
3.17.6.18 Speech 3-137
3.17.6.19 Tone 3-137
3.17.6.20 USB Backup/Restore 3-137
3.17.6.21 Voice Dialling 3-138
3.17.6.22 Web Based Management 3-138
3.17.6.23 No Tracing for All Services 3-139
3.17.7 QoS Reports 3-140
3.17.7.1 Conditions and Thresholds for Report Generation 3-140
3.17.7.2 View Report 3-143
3.17.8 Core dump 3-147

3.17.9 Remote Tracing - Syslog (V1R4.x upwards) 3-147
3.17.10 Test Interface 3-148
3.18 Bluetooth 3-149

4 Examples and HowTos. 4-1
4.1 Canonical Dialing 4-1
4.1.1 Canonical Dialing Settings 4-1
4.1.2 Canonical Dial Lookup 4-2
4.1.2.1 Conversion examples 4-3
4.2 How to Create Logo Files for OpenStage Phones 4-5
4.2.1 For OpenStage 40 4-5
4.2.2 For OpenStage 60/80 4-6
4.3 How to Set Up the Corporate Phonebook (LDAP) 4-9
4.3.1 Prerequisites: 4-9
4.3.2 Create an LDAP Template 4-10
4.3.3 Load the LDAP Template into the Phone 4-13
4.3.4 Configure LDAP Access 4-14
4.3.5 Test 4-14

5 Technical Reference 5-1
5.1 Menus 5-1
5.1.1 Web Interface Menu 5-1
5.1.1.1 Menu Structure 5-1
5.1.1.2 Web Pages 5-4
5.1.2 Local Phone Menu 5-31

Glossary 6-1

Index 7-1

1 Overview

1.1 Important Notes

Do not operate the equipment in environments where there is a danger of explosions.

For safety reasons the phone should only be operating using the supplied plug in power unit.

Use only original Siemens accessories!

Using other accessories may be dangerous, and will invalidate the warranty, extended manufacturer's liability and the CE mark.

Never open the telephone or add-on equipment. If you encounter any problems, contact System Support.

Installation requirement for USA, Canada, Norway, Finland and Sweden: Connection to networks which use outside cables is prohibited. Only in-house networks are permitted.

For USA and Canada only:
This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

This product is a UL Listed Accessory, I.T.E., in U.S.A. and Canada.
This equipment also complies with the Part 68 of the FCC Rules and the Industrie Canada CS-03.

1.2 Maintenance Notes

Do not operate the telephone in environments where there is a danger of explosions.

Use only original Siemens accessories. Using other accessories may be dangerous, and will invalidate the warranty and the CE mark.

Never open the telephone or a key module. If you encounter any problems, contact System Support.

1.3 Product Identification

1.4 About the Manual

The instructions within this manual will help you in administering and maintaining the OpenStage phone. The instructions contain important information for safe and proper operation of the phones. Follow them carefully to avoid improper operation and get the most out of your multi-function telephone in a network environment.

This guide is intended for service providers and network administrators who administer VoIP services using the OpenStage phone and who have a fundamental understanding of SIP. The tasks described in this guide are not intended for end users. Many of these tasks affect the ability of a phone to function on the network and require an understanding of IP networking and telephony concepts.

These instructions are laid out in a user-oriented manner, which means that you are led through the functions of the OpenStage phone step by step, wherever expedient. For the users, a separate manual is provided.

You can find further information on the official Siemens Enterprise Communications website (http://www.enterprise-communications.siemens.com) and on the Siemens Enterprise Wiki (http://wiki.siemens-enterprise.com).

1.5 Conventions for this Document

The terms for parameters and functions used in this document are derived from the web interface (WBM). In some cases, the the phone's local menu uses shorter, less specific terms and abbreviations. In a few cases the terminologies differ in wording. If so, the local menu term is added with a preceding "/".

1.6 The OpenStage Family

1.6.1 OpenStage 60/80

1.6.2 OpenStage 40

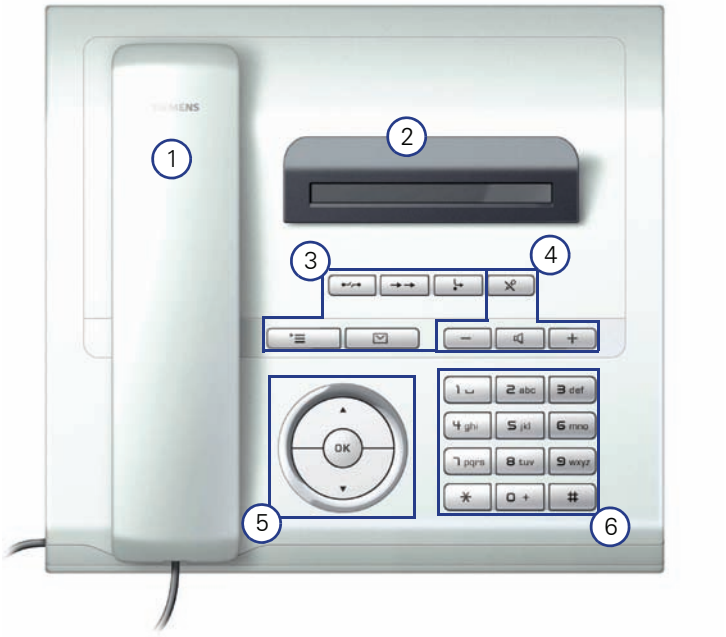
1	The **Handset** lets you pick up and dial calls in the usual manner.
2	The **Graphics Display** provides intuitive support for telephone operation.
3	The user-friendly **Application Keys** provide easy access to your telephone's applications.
4	With the **TouchGuide**, the user/administrator can navigate in the various phone functions, applications, and configuration menus.
5	You can customize your telephone in line with your personal needs by assigning individual phone numbers and functions to the **Program Keys**.
6	Press the **Function Keys** to access frequently used telephony functions.
7	The **Audio Keys** let you optimize the audio settings on your telephone.
8	With the **TouchSlider**, the user can adjust the volume, e.g. of ringtones.
9	Inbound calls are visually signaled on the **Call Display**.
10	The **Keypad** is used for entering phone numbers and text.

Tabelle 1-1

1	The **Handset** lets you pick up and dial calls in the usual manner.
2	The **Graphics Display** provides intuitive support for telephone operation.
3	The user-friendly **Application Keys** provide easy access to your telephone's applications.
4	With the **Navigation Key**, the user/administrator can navigate in the various phone functions, applications, and configuration menus.

5	You can customize your telephone in line with your personal needs by assigning individual phone numbers and functions to the **Program Keys**.
6	Press the **Function Keys** to access frequently used telephony functions.
7	The **Audio Keys** let you optimize the audio settings on your telephone.
8	Inbound calls are visually signaled on the **Call Display**.
9	The **Keypad** is used for entering phone numbers and text.

1.6.3 OpenStage 20



1	The **Handset** lets you pick up and dial calls in the usual manner.
2	The **Display** provides intuitive support for telephone operation.
3	The user-friendly **Application Keys** provide easy access to your telephone's applications.
4	Press the **Function Keys** to access frequently used telephony functions.
5	With the **Navigation Key**, the user/administrator can navigate in the various phone functions, applications, and configuration menus.
6	The **Keypad** is used for entering phone numbers and text.

1.7 Administration Interfaces

You can configure the OpenStage phone by using any of the following methods.

1.7.1 Web-based Management (WBM)

This method employs a web browser for communication with the phone via HTTP or HTTPS. It is applicable for remote configuration of individual IP phones in your network. Direct access to the phone is not required.

To use this method, the phone must first obtain IP connectivity.

1.7.2 DLS Service (Deployment Service)

The Deployment Service (DLS) is a HiPath Management application for administering phones and soft clients in both HiPath and non-HiPath networks. It has a Java-supported, web-based user interface, which runs on an internet browser. For further information, please refer to the Deployment Service Administration Guide.

1.7.3 Local Phone Menu

This method provides direct configuration of an the OpenStage phone. Direct access to the phone is required.

As long as the IP connection is not properly configured, you have to use this method to set up the phone.

2 Startup

2.1 Prerequisites

The OpenStage phone acts as an endpoint client on an IP telephony network, and has the following network requirements:

- An Ethernet connection to a network with SIP clients and servers.

> ⚠ Only use **switches** in the LAN, to which the OpenStage phone is connected. An operation at hubs can cause serious malfunctions in the hub and in the whole network.

- HiPath 8000 server.
- An FTP Server for file transfer, e. g. firmware, configuration data, application software.
- A DHCP (Dynamic Host Configuration Protocol) server (recommended).
- DLS (Deployment Service) for advanced configuration and software deployment (recommended).

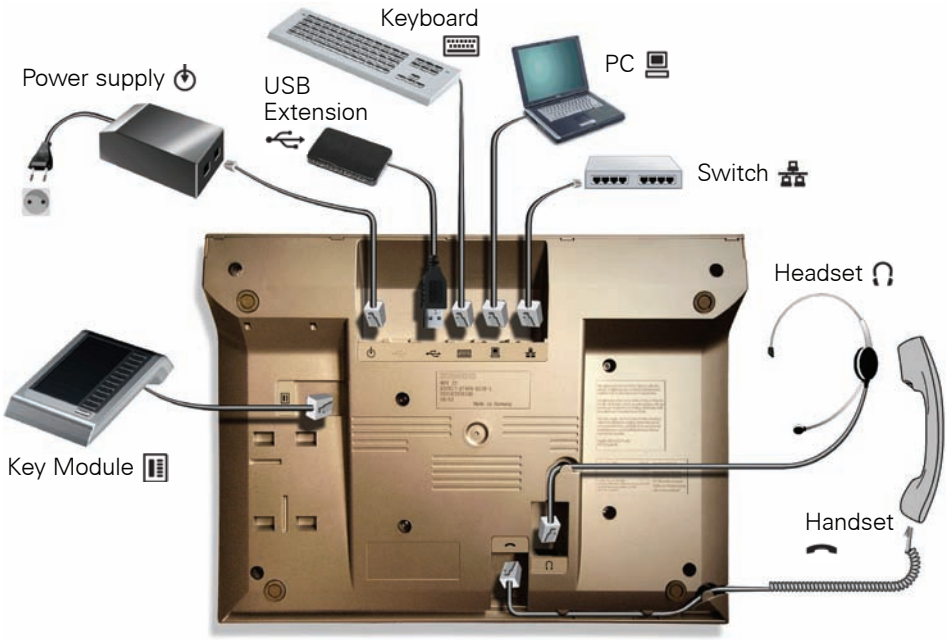
2.2 Assembling and Installing the Phone

2.2.1 Shipment

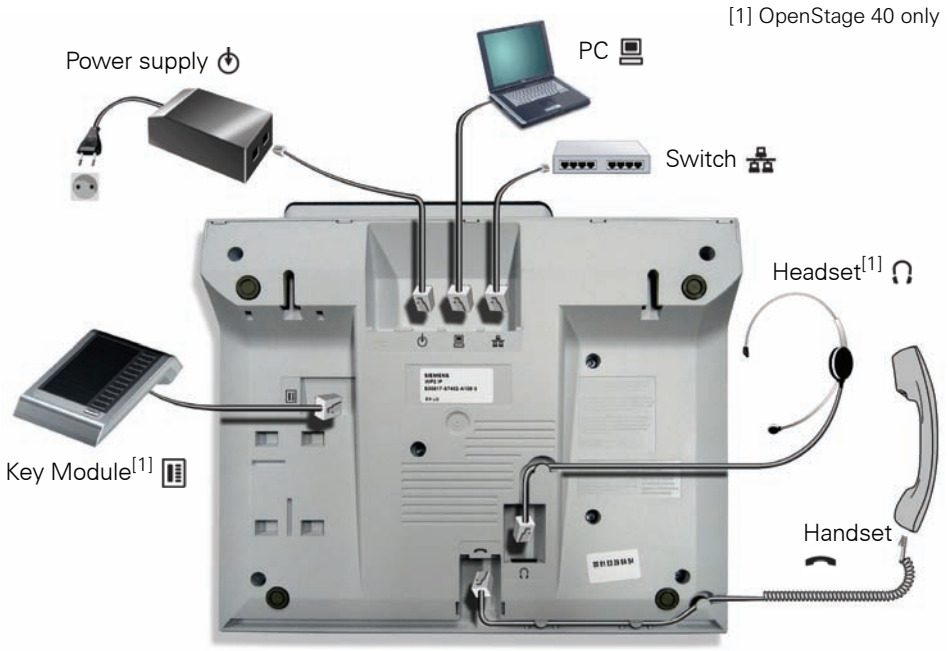
- **Phone**
- **Handset**
- **Handset cable**
- Subpackage:
  - **Document "Information and Important Operating Procedures"**
  - **Emergency number sticker**
- **Emergency Number Sticker**

2.2.2 Connectors at the bottom side

OpenStage 60



OpenStage 40 (similar to OpenStage 20, except [1])



2.2.3 Assembly

1. Handset

Insert the plug on the long end of the handset cable into the jack on the base of the telephone and press the cable into the groove provided for it. Next, insert the plug on the short end of the handset cable into the jack on the handset.

2. Emergency Number Sticker

Write your telephone number and those for the fire and police departments on the included label and attach it to the telephone housing underneath the handset (see arrow).

2.2.4 Connecting the Phone

1. Plug the LAN cable into the connector at the bottom of the telephone and connect the cable to the LAN resp. switch. If PoE (Power over Ethernet) is to be used, the PSE (Power Sourcing Equipment) must meet the IEEE 802.3af specification.
   For details about the required power supply, see the following table:

Model	**Power Consumption/Supply**
OpenStage 20	Power Class 1
OpenStage 20 G	Power Class 2
OpenStage 40[1]	Power Class 2
OpenStage 40 + 2nd Key Module	Power Class 3
OpenStage 40 G[1]	Power Class 3
OpenStage 40 G + 2nd Key Module	External power unit required
OpenStage 60/80[2]	Power Class 3
OpenStage 60/80 + 2nd Key Module	Power Class 3
OpenStage 60/80 G[2]	Power Class 3
OpenStage 60/80 G + 2nd Key Module	External power unit required

Tabelle 2-1

1 Includes 1 Key Module.
2 Includes 1 Key Module + USB-Extension with Acoustic Unit.

2. Only if Power over Ethernet (PoE) is **NOT** supported:

> Use only the plug-in power supply unit fitting the OpenStage phone:
> EU: C39280-Z4-C510
> UK: C39280-Z4-C512
> USA: C39280-Z4-C511

Plug the power supply unit into the mains. Connect the plug-in power supply unit to the jack at the bottom of the phone.

3. If applicable, connect the following optional jacks:
   - LAN connection to PC
   - Headset (accessory)
   - Connection to add-on device (accessory)
   - Connection to external keyboard (accessory)
   - USB master for connection to a USB device (e. g. accessory USB Acoustic Adapter)

To prevent damage on the OpenStage phone, connect an USB stick using the adapter cable C39195-Z7704-A5.

Do not connect a USB hub to the phone's USB port, as this may lead to stability problems.

2.3 Quick Start

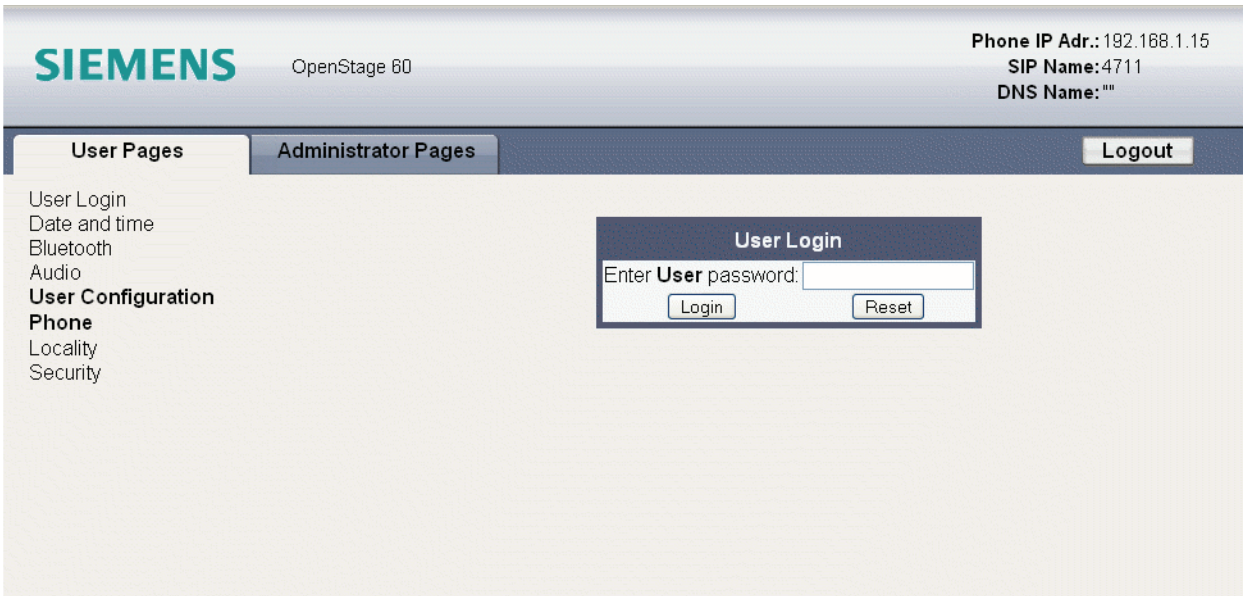
This section describes a typical case: the setup of an OpenStage endpoint in an environment using a DHCP server and the web interface. For different scenarios, cross-references to the corresponding section of the administration chapter are given.

Alternatively, the DLS (Deployment Service) administration tool can be used. Its Plug & Play functionality allows to provide the phone with configuration data by assigning an existing data profile to the phone's MAC address or E.164 number. For further information, see the Deployment Service Administration Manual.

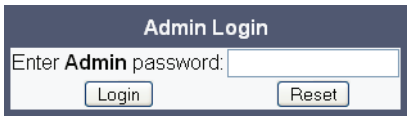
Any settings made by a DHCP server are not configurable by other configuration tools.

2.3.1 Access the Web Interface (WBM)

1. Open your web browser (MS Internet Explorer or Firefox) and enter the transfer protocol, IP address and port number of your phone. If HTTP is used, port 8085 must be added, for example http://192.168.1.15:8085. For HTTPS, the phone uses the standard port 443.
   After entering the URL, the browser might display a certificate notification. The start page of the web interface appears. In the upper right corner, the phone number, the phone's IP address, as well as the DNS name assigned to the phone are displayed. The left corner contains the user menu tree.



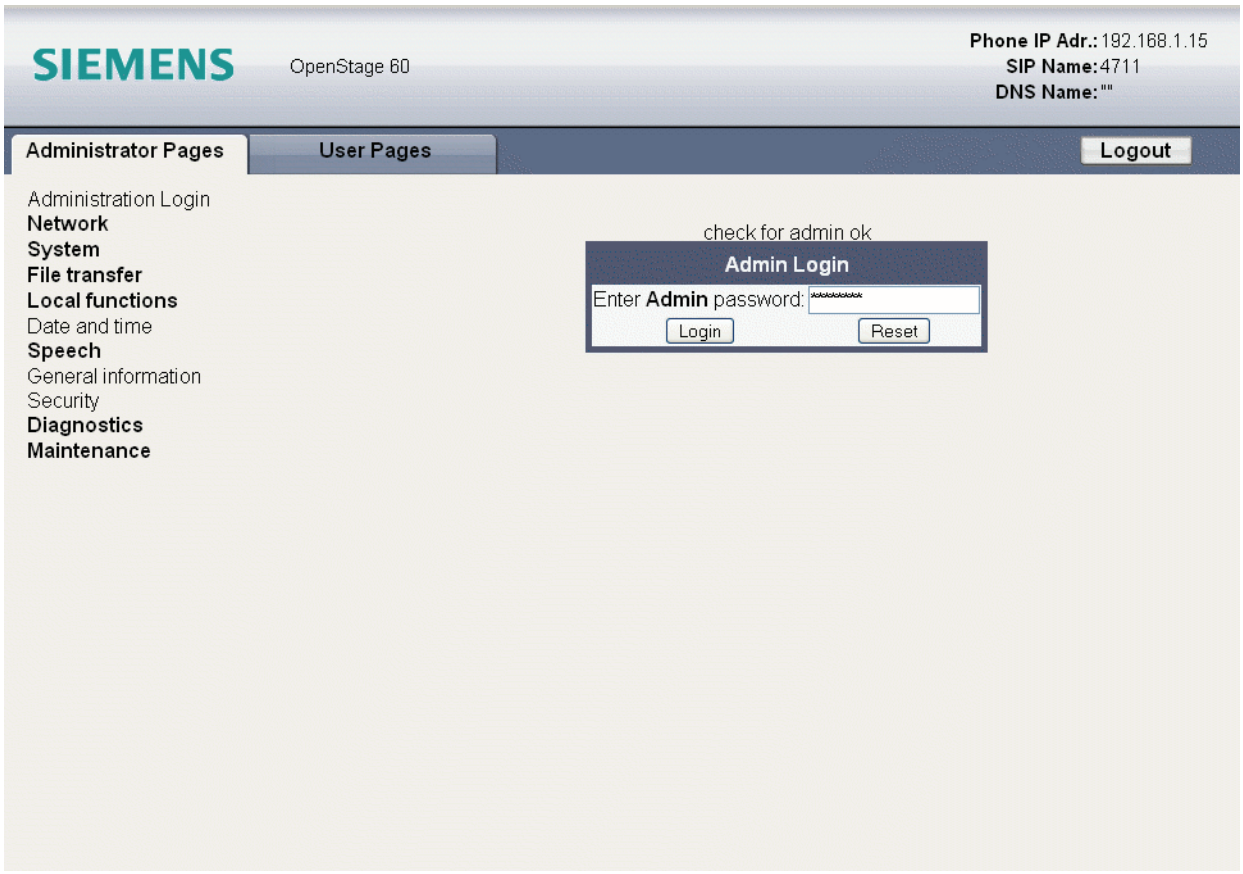
2. Click on the tab "Administrator Pages". In the dialog box, enter the admin password:



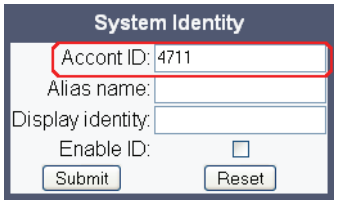
3. The administration main page opens. The left column contains the menu tree. If you click on an item which is printed in normal style, the corresponding dialog opens in the center of the page. If you click on an item printed in bold letters, a sub-menu opens in the right column.

2.3.2 Set the Terminal Number

If the user and administrator menus are needed in the course of setup, the terminal number, which by default is identical with the phone number, must be configured first. The terminal number input form is presented to the user/administrator right after booting, unless the Plug&Play facility of the DLS is used. For further information about this setting, please refer to Section 3.5.1.1, “Terminal Identity”. With the WBM, the teminal number is configured as follows:



4. In the left column, select System > System Identity to open the "System Identity" dialog. Enter the terminal number, i. e. the SIP name / phone number.



2.3.3 Basic Network Configuration

For basic functionality, DHCP must provide the following parameters:

- **IP Address**: IP Address for the phone.
- **Subnet Mask (option #1)**: Subnet mask of the phone.
- **Default Route (option #3 "Router")**: IP Address of the default gateway which is used for connections beyond the subnet.
- **DNS IP Addresses (option #6 "Domain Server")**: IP Addresses of the primary and secondary DNS servers.

If no DHCP server is present, see Section 3.3.3, “IP Address - Manual Configuration” for IP address and subnet mask, and Section 3.3.4, “Default Route/Gateway” for default route.

2.3.4 Date and Time / SNTP

An SNTP (Simple Network Time Protocol) server provides the current date and time for network clients. The IP address of an SNTP server can be given by DHCP.

In order to provide the correct time, it is required to give the timezone offset, i.e. the shift in hours to be added to the UTC time provided by the SNTP server.

The following DHCP options are required:

- **SNTP IP Address (option #42 "NTP Servers")**: IP Address of the SNTP server to be used by the phone.
- **Timezone offset (option #2 "Time Offset")**: Offset in hours in relationship to the UTC time provided by the SNTP server.

For manual configuration of date and time see Section 3.5.4, “Date and Time”.

2.3.5 SIP Server Address

The IP Address or hostname of a SIP server can be provided by DHCP.

The option’s name and code are as follows:

- **option #120 "SIP Servers DHCP Option"**

For manual configuration of the SIP server address see Section 3.5.5.1, “SIP Addresses”.

2.3.6 Extended Network Configuration

To have constant access to other subnets, you can enter a total of two more network destinations. For each further domain/subnet you wish to use, first the IP address for the destination, and then that of the router must be given. The option's name and code are as follows:

- **option #33 "Static Routing Table"**

For manual configuration of specific/static routing see Section 3.3.5, "Specific IP Routing".

Also the DNS domain wherein the phone is located can be specified by DHCP. The option's name and code are as follows:

- **option #15 "Domain Name"**

For manual configuration of the DNS domain name see Section 3.3.6.1, "DNS Domain Name".

2.3.7 Vendor specific: VLAN Discovery and DLS address

If the phone is to be located in a VLAN (Virtual LAN), a VLAN ID must be assigned. In case the VLAN shall be provided by DHCP, **VLAN Discovery** must be set to "DHCP" (see Section 3.2.2.1, "Automatic VLAN discovery (DHCP)").

If a DLS (Deployment Service) server is in use, its IP address must be provided. It is recommended to configure the DLS server address by DCHP, as this method enables full Plug & Play: having received the DLS address from DHCP, the phone will contact the DLS during startup. Provided that the DLS is configured appropriately, it will send all necessary configuration data to the phone. Additionally, this method is relevant to security, as it ensures the authenticity of the DLS server.

For manual configuration of the DLS server address see Section 3.3.7, "Configuration & Update Service (DLS)".

For the configuration of vendor-specific settings by DHCP, there are two alternative methods: 1) the use of a vendor class, or 2) the use of DHCP option 43.

2.3.7.1 Using a Vendor Class

It is recommended to define a vendor class on the DHCP server, thus enabling server and phone to exchange vendor-specific data exclusively. The data is disclosed from other clients.

In the following, the configuration of vendor classes is explained both for a Windows DHCP Server and for Unix/Linux.

Configuration of the Windows DHCP Server

For DHCP servers on a pre-SP2 Windows 2003 Server:

Windows 2003 Server contains a bug that prevents you from using the DHCP console to create an option with the ID 1 for a user-defined vendor class. Instead, this entry must be created with the `netsh` tool in the command line (DOS shell).

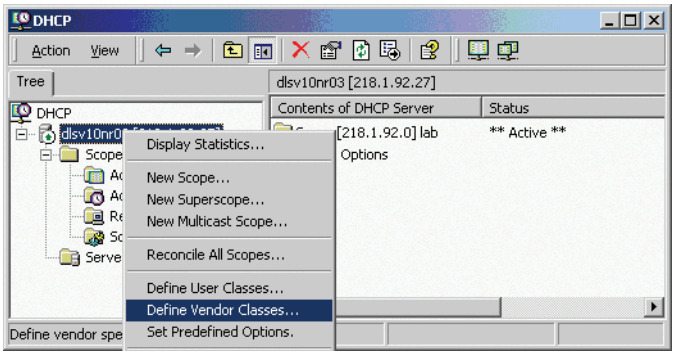
You can use the following command to set the required option (without error message), so that it will appear in the DHCP console afterwards:

```
netsh dhcp server add optiondef 1 "Optipoint element 001"
STRING 0 vendor=OptiIpPhone comment="Tag 001 for Optipoint"
```

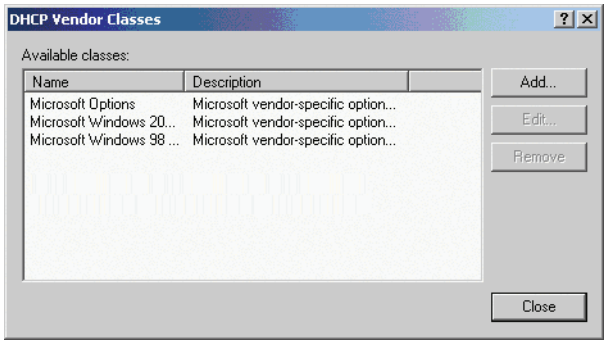
The value "Siemens" for optiPoint Element 1 can then be re-assigned using the DHCP console.

This error was corrected in Windows 2003 Server SP2.

1. In the Windows Start menu, select **Start** > **Programs** > **Administrative Tools** > **DHCP**.
2. In the DHCP console menu, right-click the DHCP server in question and select **Define Vendor Classes...** in the context menu.

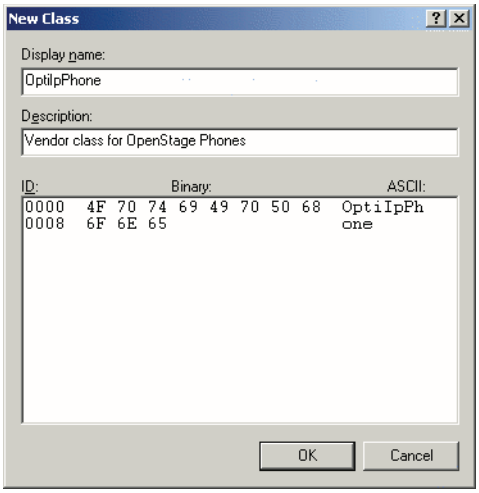


3. A dialog window opens with a list of the classes that are already available.

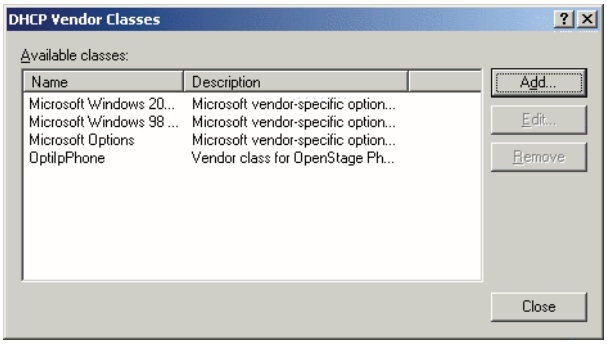


4. Press **Add...** to define a new vendor class.

5. Enter "OptiIpPhone" as **Display name** and give a description of this class. Provide the class name proper by setting the cursor underneath **ASCII** and typing "OptiIpPhone". The binary value is displayed simultaneously.

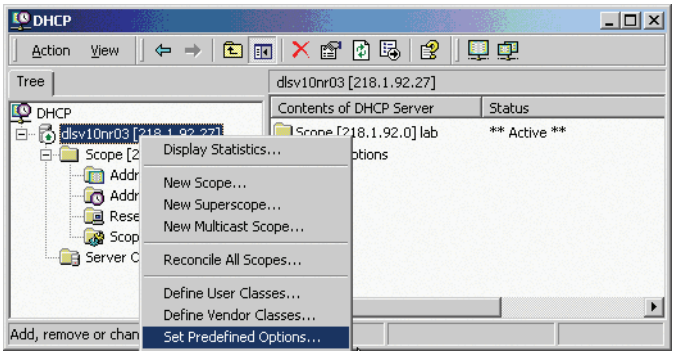


Click **OK** to apply the changes. The new vendor class now appears in the list:

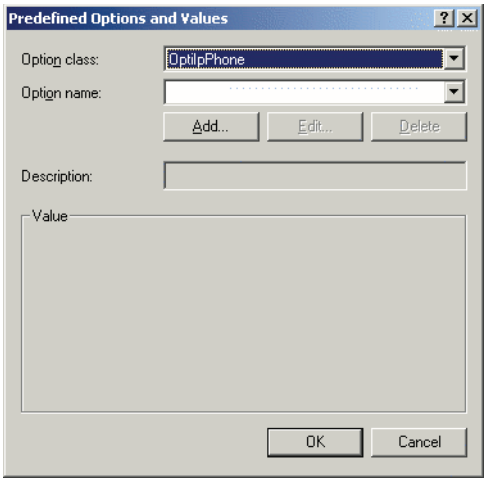


6. Exit the window with **Close**.

7. In the DHCP console menu, right-click the DHCP server in question and select **Set Predefined Options** from the context menu.

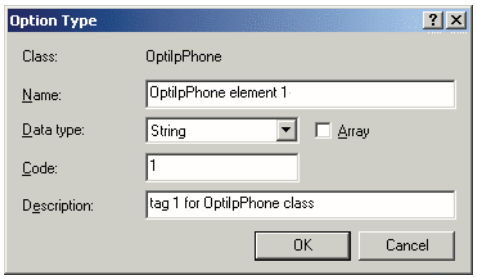


8. In the dialog, select the previously defined **OptiIpPhone** class and click on **Add...** to add a new option. (If the workaround for a pre-SP2 Windows 2003 Server has been applied, the first option will be there already.)



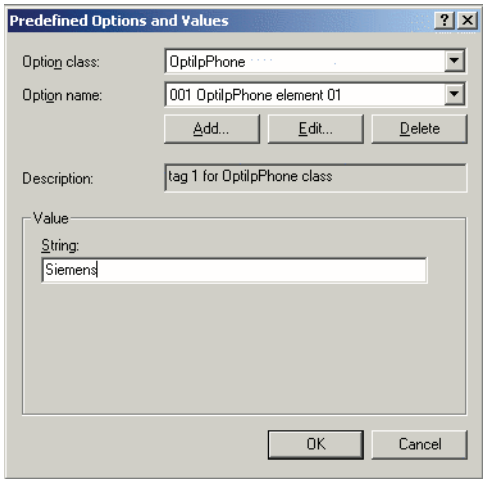
9. In the following dialog, specify the option type as follows. (If the workaround for a pre-SP2 Windows 2003 Server has been applied, the option type dialog will be skipped for the first option.)

   - **Name:** Free text, e. g. "OptiIpPhone element 01".
   - **Data type:** "String".
   - **Code:** "1"**.**
   - **Description:** Free text, e. g. "tag 1 for OptiIpPhone class".



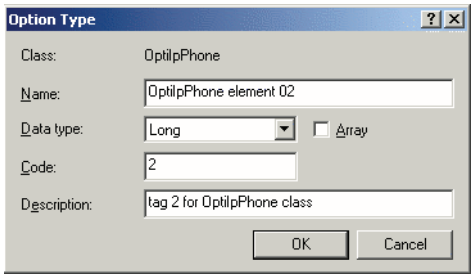
Click **OK** to return to the previous window.

10. The newly created option is displayed now. Enter "Siemens" in the **Value** field.



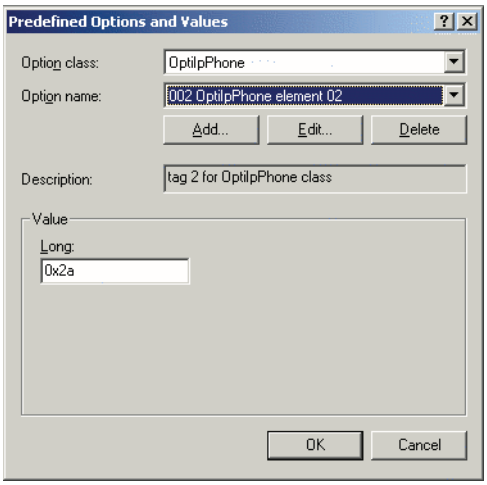
11. If the VLAN is to be provided by DHCP: Repeat step 7 and 8, and then specify the option type as follows. If you want to proceed to the configuration of the DLS address, continue with step 13.

    - **Name:** Free text, e. g. "OptiIpPhone element 02"
    - **Data type:** "Long"
    - **Code:** "2"
    - **Description:** Free text, e. g. "tag 2 for OptiIpPhone class".



    Click **OK** to return to the previous window.

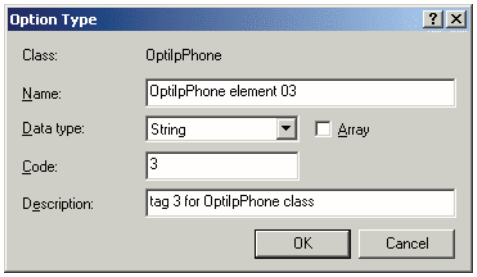
12. The newly created option is displayed now. Enter the VLAN ID as a hexadecimal number in the **Value** field. In the example, the VLAN ID is 10 (Hex: 2A).



    If you do not intend to configure the DLS address, click OK and continue with step 15.

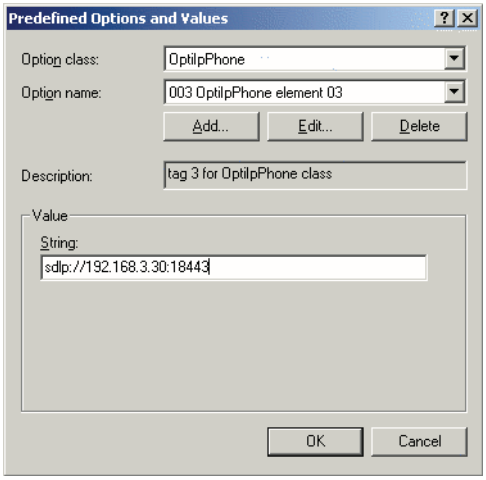
13. If the DLS address is to be provided by DHCP: Repeat step 7 and 8, and then specify the option type as follows.

    - **Name:** Free text, e. g. "OptiIpPhone element 03".
    - **Data type:** "String".
    - **Code:** "3"**.**
    - **Description:** Free text, e. g. "tag 3 for OptiIpPhone class".



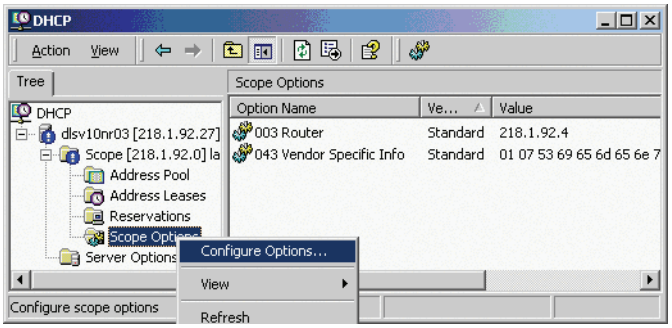
Click **OK** to return to the previous window.

14. The newly created option is displayed now. Enter the DLS address in the **Value** field, using the following format:
<PROTOCOL>:://<IP ADDRESS OF DLS SERVER>:<PORT NUMBER>
In the example, the DLS address is "sdlp://192.168.3.30:18443".

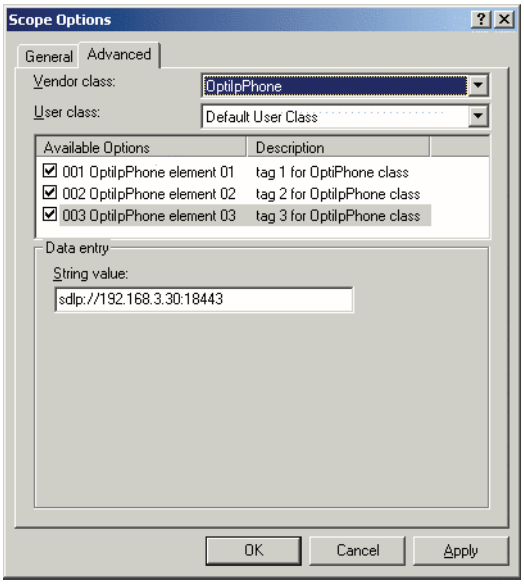


Click **OK**.

15. To define a scope, select the DHCP server in question, and then **Scope**, and right-click **Scope Options**. Select **Configure Options...** in the context menu.

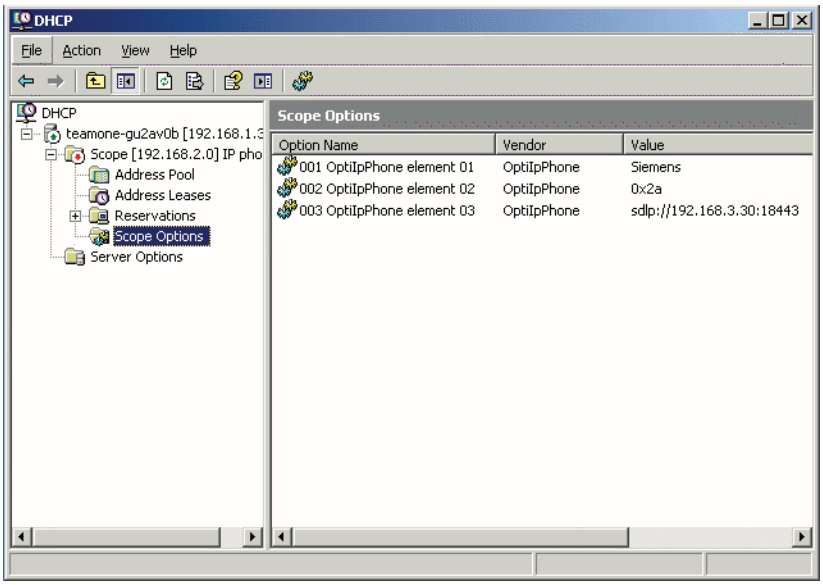


16. Select the **Advanced** tab. Under **Vendor class**, select the class that you previously defined (**OptiIpPhone**) and, under **User class**, select **Default User Class**.



Activate the check boxes for the options that you want to assign to the scope (in the example, **001**, **002**, and **003**). Click **OK**.

17. The DHCP console now shows the information that will be transmitted to the corresponding workpoints. Information from the **Standard** vendor is transmitted to all clients, whereas information from the **OptiIpPhone** vendor is transmitted only to the clients (workpoints) in this vendor class.



Setup using a DHCP server on Unix/Linux

The following snippet from a DHCP configuration file (usually dhcpd.conf) shows how to set up a configuration using a vendor class and the "vendor-encapsulated-options" option.

```
class "OptiIpPhone" {
   option vendor-encapsulated-options
   # The vendor encapsulated options consist of hexadecimal values for
the option number (for instance, 01), the length of the value (for in-
stance, 07), and the value (for instance, 53:69:65:6D:65:6E:73). The
options can be written in separate lines; the last option must be fol-
lowed by a ';' instead of a ':'.
   # Tag/Option #1: Vendor "Siemens"
   #1  7  S  i  e  m  e  n  s
    01:07:53:69:65:6D:65:6E:73:
   # Tag/Option #2: VLAN ID
   # 2  4  0  0  0 10
    02:04:00:00:00:0A;
   # Tag/Option #3: DLS IP Address (here: sdlp://192.168.3.30:18443)
   # 3 25 s  d  l  p  :  / /  1  9  2  .  1  6  8  .  3  . (...etc.)
    03:19:73:64:6C:70:3A:2F:2F:31:39:32:2E:31:36:38:2E:33:2E:33:30:
3A:31:38:34:34:33;
   match if substring (option vendor-class-identifier, 0, 11) =
   "OptiIpPhone";
}
```

2.3.7.2 Using Option #43 "Vendor Specific"

Alternatively, option #43 can be used for setting up the VLAN ID and DLS address. The following tags are used:

- **Tag 1: Vendor name**
- **Tag 2: VLAN ID**
- **Tag 3: DLS address**

Optionally, the DLS address can be given in an alternative way:

- **Tag 4: DLS hostname**

The Vendor name tag is coded as follows (the first line indicates the ASCII values, the second line contains the hexadecimal values):

Code	**Length**	**Vendor name**						
1	7	S	i	e	m	e	n	s
01	07	53	69	65	6D	65	6E	73

Table 2-2

The following example shows a VLAN ID with the decimal value "10". Providing

Code	**Length**	**VLAN ID**			
2	4	0	0	1	0
02	04	00	00	00	0A

Table 2-3

For manual configuration of the VLAN ID see Section 3.2.2.2, “Manual configuration of a VLAN ID”.

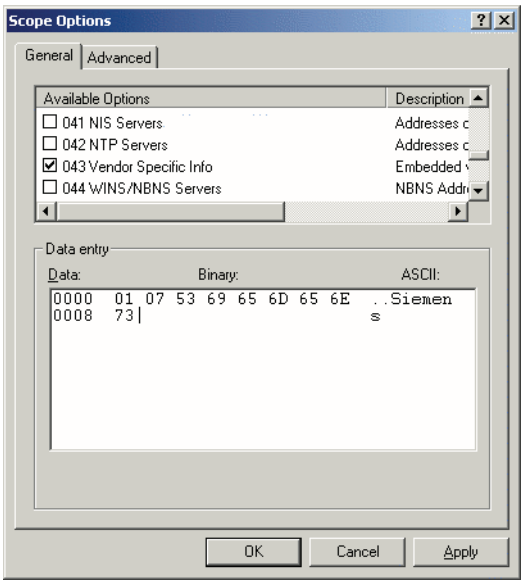
The DLS IP address tag consists of the protocol prefix "sdlp://", the IP address of the DLS server, and the DLS port number, which is "18443" by default. The following example illustrates the syntax:

Code	**Length**	**DLS IP address**																							
3	25	s	d	l	p	:	/	/	1	9	2	.	1	6	8	.	3	.	3	0	:	1	8	4	4	3
03	19	73	64	6C	70	3A	2F	2F	31	39	32	2E	31	36	38	2E	33	2E	33	30	3A	31	38	34	34	33

Setup using the Windows DHCP Server

1. In the Windows Start menu, select **Start** > **Programs** > **Administrative Tools** > **DHCP**.
2. Select the DHCP server and the scope. Choose **Configure Options** in the context menu using the right mouse button.

3. Enter tag 1, that is the vendor tag.

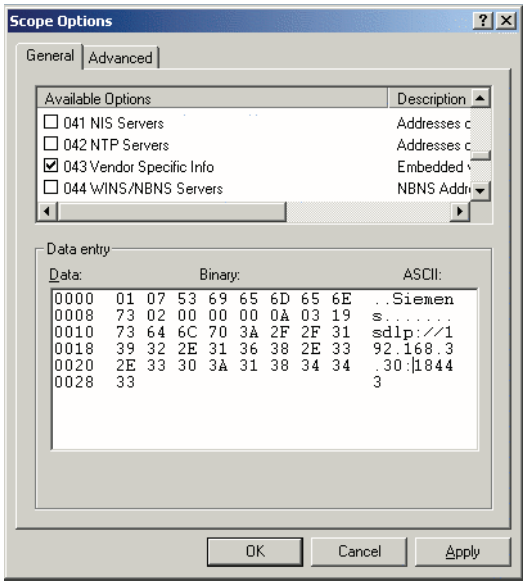


4. If the VLAN ID is to be provided by DHCP: Enter the hexadecimal value in **Data entry**. Providing the length is not required here, as the VLAN ID is always 4 Bytes long. In the example, the VLAN ID is 10 (Hex: 2A).

5. If the DLS address is to be provided by DHCP: Enter the DLS address in the **Value** field, using the following format:
<PROTOCOL>:://<IP ADDRESS OF DLS SERVER>:<PORT NUMBER>

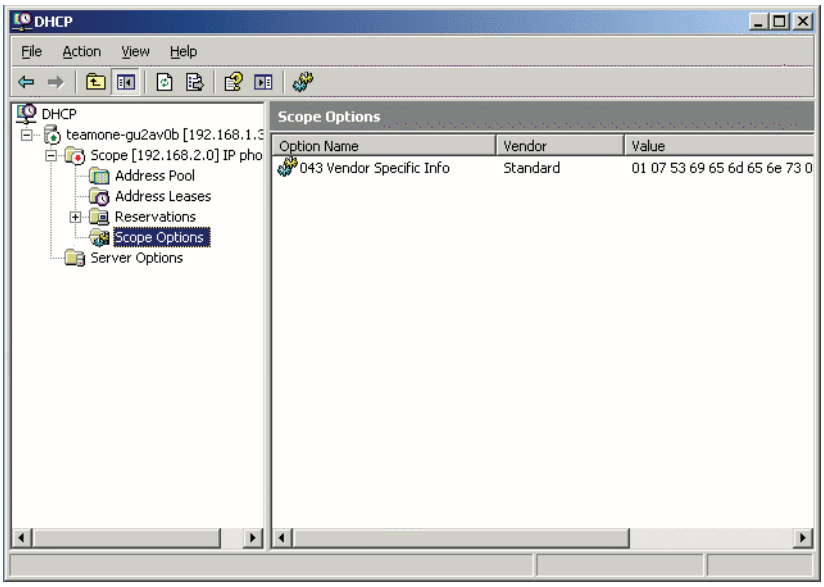
> For ensuring proper functionality, the port number should not be followed by any character.

In the example, the DLS address is "sdlp://192.168.3.30:18443".
Note that the screenshot also shows the VLAN ID described in step 4.



Click **OK**.

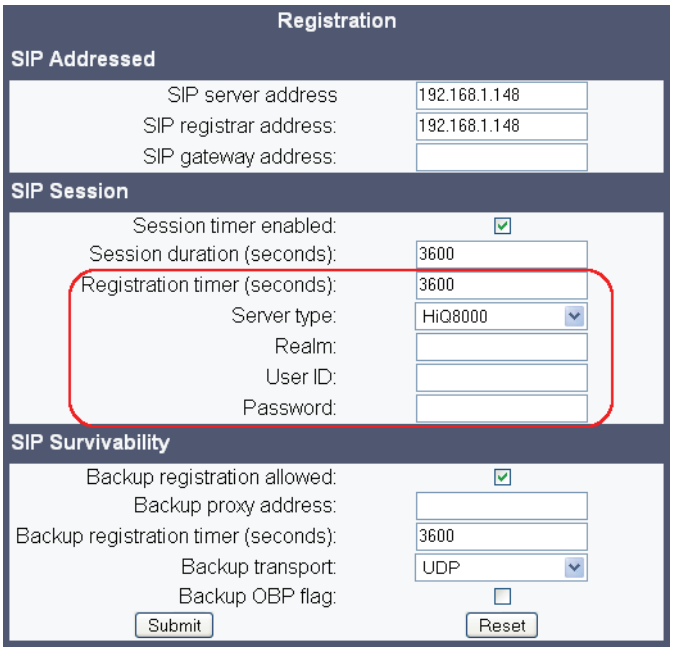
6. The DHCP console now shows the information that will be transmitted to the corresponding workpoints.



2.3.8 Registering at the HiPath 8000

For registration at the HiPath 8000 SIP server, a SIP user ID and passwort must be provided by the phone. The following procedure describes the configuration using the web interface (see Section 2.3.1, “Access the Web Interface (WBM)”; if the web interface is not applicable, please refer to Section 3.5.6, “Authenticated Registration”):

1. In the administration menu, select System > Registration. The "Registration" dialog opens.



2. In the **Server type** field, enter "HiQ8000".
3. In **Realm**, enter the SIP realm the targeted user/password combination refers to.
4. In the **User ID** and **Password** fields, enter the user name/password combination for the phone.

3 Administration

This chapter describes the configuration of every parameter available on the OpenStage phones. For access via the local phone menu, see the following; for access using the web interface, please refer to Section 2.3.1, “Access the Web Interface (WBM)”.

3.1 Access via Local Phone

The data entered in input fields is parsed and controlled by the phone. Thus, data is accepted only if it complies to the value range.

1. **Access the Administration Menu**

   OpenStage 60/80:

   Press the ☰ key to activate the administration menu (the ☰ key toggles between the user’s configuration menu and the administration menu).

   OpenStage 60/80 V1R3.x upwards:

   The ☰ key toggles between the Settings menu, the Applications menu, and the applications currently running. Press the ☰ key repeatedly until the "Settings" tab is active. (The ☰ key toggles between the Settings menu, the Applications menu, and the applications currently running.)

   OpenStage 20/40:

   Press the keys ☰, ▼, and OK consecutively to select the administration menu.

2. **Enter Password**

   When the Admin menu is active, you will be prompted to enter the administrator password. The default admin password is "123456". It is recommended to change the password (see Section 3.14, “Password”) after your first login.

   For entering passwords with non-numeric characters, please consider the following:

   By default, password entry is in numeric mode. For changing the mode, press the # key once or repeatedly, depending on the desired character. The # key cycles around the input modes as follows:

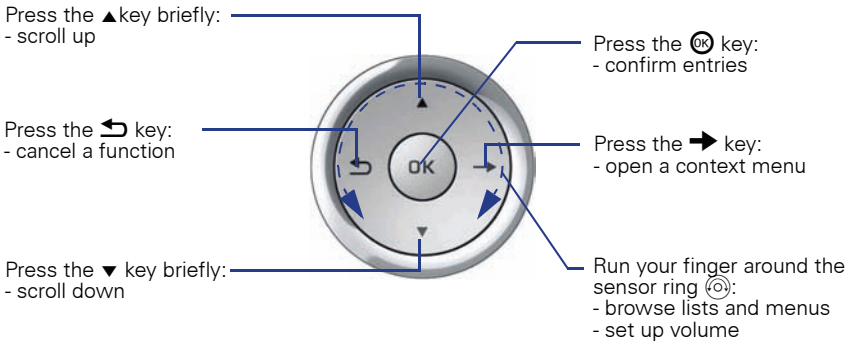
   (Abc) -> (abc) -> (123) -> (ABC) -> back to start.

3. Navigate within the Administration Menu

OpenStage 60/80

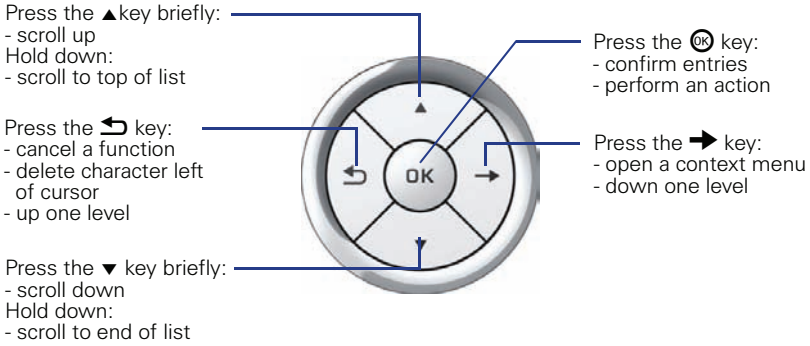
Use the TouchGuide to navigate and execute administrative actions in the administration menu.

For using the TouchGuide, see the following figure:


Press the ▲key briefly:
- scroll up
Press the ⮌ key:
- cancel a function
Press the ▼ key briefly:
- scroll down
OK
Press the OK key:
- confirm entries
Press the ➔ key:
- open a context menu
Run your finger around the sensor ring:
- browse lists and menus
- set up volume

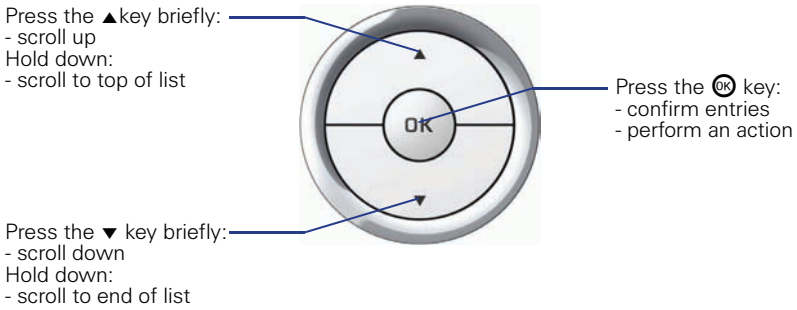
OpenStage 40

Use the 5-way Navigator to navigate and execute administrative actions in the administration menu.



OpenStage 20

Use the 3-way Navigator to navigate and execute administrative actions in the administration menu.



4. Select a parameter

If a parameter is set by choosing a value from a selective list, an arrow symbol appears in the parameter field that has the focus. Press the key to enter the selective list. Use the Sensor Wheel resp. the ▲ and ▼ key to scroll up and down in the selective list. To select a list entry, press the OK key.

5. Enter the parameter value

For selecting numbers and characters, you can use special keys. See the following table:

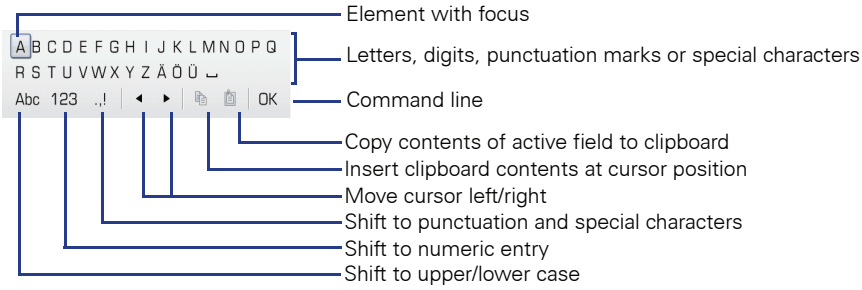
Key	Function
*	Switch to punctuation and special characters.
#	Toggle between lowercase characters, uppercase characters, and digits in the following order: (Abc) -> (abc) -> (123) -> (ABC) -> back to start.

Tabelle 3-1

OpenStage 60/80

If a parameter is set by entering a number or character data, the onscreen keypad is used. Press the OK key to enter the editor. Within the editor, solely use the key numbers or the Sensor Wheel for selecting numbers, characters, or groups of characters. The ⮌ key deletes one character in the input field, and the ➔ key moves the cursor to the OK field.

The following figure describes the elements of the onscreen keypad and their functions:


Element with focus
A B C D E F G H I J K L M N O P Q
R S T U V W X Y Z Ä Ö Ü ␣
Abc 123 .,! OK
Letters, digits, punctuation marks or special characters
Command line
Copy contents of active field to clipboard
Insert clipboard contents at cursor position
Move cursor left/right
Shift to punctuation and special characters
Shift to numeric entry
Shift to upper/lower case

Additionally, you can use the following keys on the keypad as shortcuts for the selection of character groups

Element	Function
*🔔	Switch to punctuation and special characters.
#⊸	Toggle between lowercase characters, uppercase characters, and digits.

OpenStage 20/40

With the OpenStage 20/40, use the keypad for entering parameters. With the 3 way/5 way-Navigator, you can enter, delete, copy and paste characters and numbers as well as navigate within an entry and toggle the input mode.

6. Save and exit

When you are done, select **Save & exit** and press OK.

3.2 LAN Settings

3.2.1 LAN Port Settings

The OpenStage phone provides an integrated switch which connects the LAN, the phone itself and a PC port. By default, the switch will auto negotiate transfer rate (10/100 Mb/s, 1000 Mb/s with OpenStage 20/40/60/80 G) and duplex method (full or half duplex) with whatever equipment is connected. Optionally, the required transfer rate and duplex mode can be specified manually using the **LAN port speed** parameter.

In the default configuration, the LAN port supports automatic detection of cable configuration (pass through or crossover cable) and will reconfigure itself as needed to connect to the network. If the phone is set up to manually configure the switch port settings, the cable detection mechanism is disabled. In this case, care must be taken to use the correct cable type.

The PC Ethernet port is controlled by the **PC port mode** parameter. If set to "Disabled", the PC port is inactive; if set to "Enabled", it is active. If set to "Mirror", the data traffic at the LAN port is mirrored at the PC port. This setting is for diagnostic purposes. If, for instance, a PC running Ethereal/Wireshark is connected to the PC port, all network activities at the phone's LAN port can be captured.

When **PC port autoMDIX** is enabled, the switch determines automatically whether a regular MDI connector or a MDI-X (crossover) connector is needed, and configures the connector accordingly.

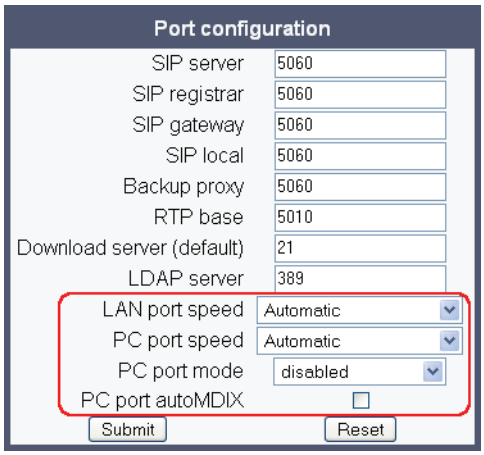
Data required

- **LAN port speed** / **LAN port type**: Settings for the ethernet port connected to a LAN switch.
  Value range: "Automatic," "10 Mbps half duplex", "10 Mbps full duplex", "100 Mbps half duplex", "100 Mbps full duplex", "1 Gbps half duplex" (OpenStage 60/80 G), "1 Gbps full duplex" (OpenStage 60/80 G).
  Default: "Automatic".
- **PC port speed** / **PC port type**: Settings for the ethernet port connected to a PC.
  Value range: "Automatic", "10 Mbps half duplex", "10 Mbps full duplex", "100 Mbps half duplex", "100 Mbps full duplex", "1 Gbps half duplex" (OpenStage 60/80 G), "1 Gbps full duplex" (OpenStage 60/80 G).
  Default: "Automatic".
- **PC port mode** / **PC port status**: Controls the PC port.
  Value range: "disabled", "enabled", "mirror".
  Default: "disabled".

- **PC port autoMDIX**: Switches between MDI and MDI-X automatically.
  Value range: "On", "Off".
  Default: "Off".

Administration via WBM

Network > Port configuration



Administration via Local Phone

```
└--- Administration
     └--- Network
          └--- Port Configuration
               |--- LAN port type
               |--- PC port status
               |--- PC port type
               └--- PC port autoMDIX
```

3.2.2 VLAN

VLAN (Virtual Local Area Network) is a technology that allows network administrators to partition one physical network into a set of virtual networks (or broadcast domains).

Physically partitioning the LAN into separate VLANs allows a network administrator to build a more robust network infrastructure. A good example is a separation of the data and voice networks into data and voice VLANs. This isolates the two networks and helps shield the endpoints within the voice network from disturbances in the data network and vice versa.

The implementation of a voice network based on VLANs requires the network infrastructure (the switch fabric) to support VLANs.

In a layer 1 VLAN, the ports of VLAN-aware switch are assigned to a VLAN statically. The switch only forwards traffic to a particular port if that port is a member of the VLAN that the traffic is allocated to. Any device connected to a VLAN-assigned port is automatically a member of this VLAN, without being a VLAN aware device itself. If two or more network clients are connected to one port, they cannot be assigned to different VLANs. When a network client is moving from one switch to another, the switches' ports have to be updated accordingly by hand.

With a layer 2 VLAN, the assignment of VLANs to network clients is realized by the MAC addresses of the network devices. In some environments, the mapping of VLANs and MAC addresses can be stored and managed by a central database. Alternatively, the VLAN ID, which defines the VLAN whereof the device is a member, can be assigned directly to the device, e. g. by DHCP. The task of determining the VLAN an Ethernet packet is belonging to is carried out by VLAN tags within each Ethernet frame. As the MAC addresses are (more or less) wired to the devices, mobility does not require any administrator action, as opposed to layer 1 VLAN. It is possible to assign one device, i.e. one MAC address, to different VLANs.

It is important that every switch connected to a PC is VLAN-capable. This is also true for the integrated switch of the OpenStage. The phone must be configured as a VLAN aware endpoint if the phone itself is a member of the voice VLAN, and the PC connected to the phone's PC port is a member of the data VLAN.

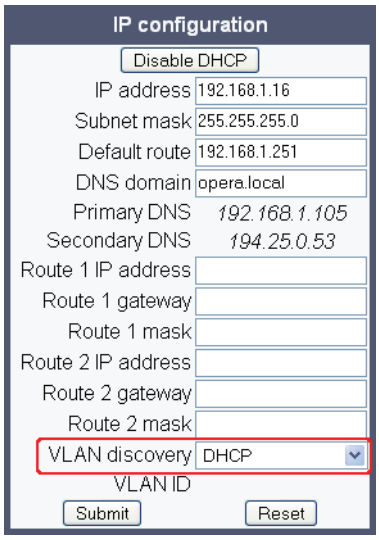
The VLAN ID can be configured automatically by DHCP or manually.

3.2.2.1 Automatic VLAN discovery (DHCP)

To automatically discover a VLAN ID using DHCP, the phone must be configured as DHCP enabled, and **VLAN discovery** mode must be set to "DHCP". The DHCP server must be configured to supply the Vendor Unique Option in the correct Siemens VLAN over DHCP format. If a phone configured for VLAN discovery by DHCP fails to discover its VLAN, it will proceed to configure itself from the DHCP within the non-tagged LAN. In these circumstances network routing will probably not be correct.

Administration via WBM

Network > IP configuration



Administration via Local Phone

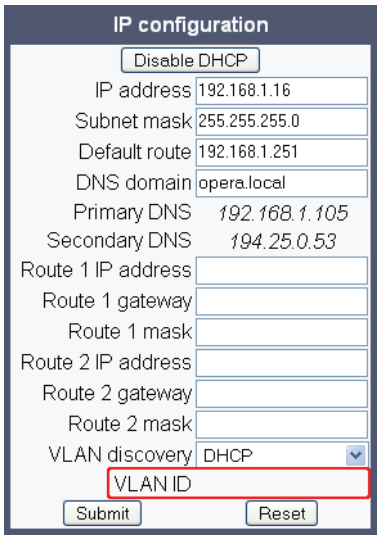
└── Administration
  └── Network
    └── IP Configuration
      └── **VLAN discovery**

3.2.2.2 Manual configuration of a VLAN ID

To configure layer 2 VLAN and QoS manually, first make shure that QoS layer 2 and 3 are configured as described in Section 3.3.1, “Quality of Service (QoS)”, and VLAN discovery is set to "Manual" (see Section 3.2.2.1, “Automatic VLAN discovery (DHCP)”). Then, the phone must be provided with a VLAN ID between 1 and 4095. If you mis-configure a phone to an incorrect VLAN, the phone will possibly not connect to the network. In DHCP mode it will behave as though the DHCP server cannot be found, in fixed IP mode no server connections will be possible.

Administration via WBM

Network > IP configuration



Administration via Local Phone

Administration
Network
IP Configuration
VLAN ID

3.3 IP Network Parameters

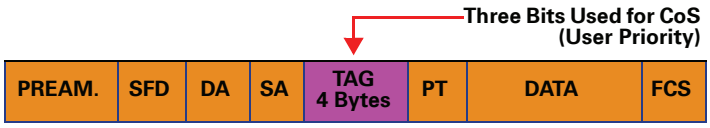
3.3.1 Quality of Service (QoS)

The QoS technology based on layer 2 and the two QoS technologies Diffserv and TOS/IP Precedence based on layer 3 are allowing the VoIP application to request and receive predictable service levels in terms of data throughput capacity (bandwidth), latency variations (jitter), and delay.

3.3.1.1 Layer 2 / 802.1p

QoS on layer 2 is using 3 Bits in the 802.1q/p 4-Byte VLAN tag which has to be added in the Ethernet header.

The CoS (class of service) value can be set from 0 to 7. 7 is describing the highest priority and is reserved for network management. 5 is used for voice (RTP-streams) by default. 3 is used for signaling by default.

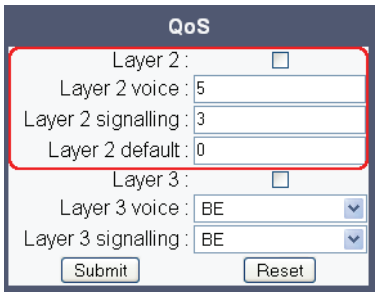


Data required

- **Layer 2**: Activates or deactivates QoS on layer 2.
  Value range: "Yes", "No".
  Default: "Yes".
- **Layer 2 voice**: Sets the CoS (Class of Service) value for voice data (RTP streams).
  Value range: 0-7.
  Default: 5.
- **Layer 2 signalling**: Sets the CoS (Class of Service) value for signaling.
  Value range: 0-7.
  Default: 3.
- **Layer 2 default**: Sets the default CoS (Class of Service) value.
  Value range: 0-7.
  Default: 0.

Administration via WBM

Network > QoS



Administration via Local Phone

```
└--- Administration
     └--- Network
          └--- QoS
               └--- Service
                    ├--- Layer 2
                    ├--- Layer 2 voice
                    ├--- Layer 2 signalling
                    └--- Layer 2 default
```

3.3.1.2 Layer 3 / Diffserv

Diffserv assigns a class of service to an IP packet by adding an entry in the IP header.

Traffic flows are classified into 3 per-hop behavior groups:

1. Default
   Any traffic that does not meet the requirements of any of the other defined classes is placed in the default per-hop behaviour group. Typically, the forwarding has best-effort forwarding characteristics. The DSCP (Diffserv Codepoint) value for Default is "0 0 0 0 0 0".
2. Expedited Forwarding (EF referred to RFC 3246)
   Expedited Forwarding is used for voice (RTP streams) by default. It effectively creates a special low-latency path in the network. The DSCP (Diffserv Codepoint) value for EF is "1 0 1 1 1 0".
3. Assured Forwarding (AF referred to RFC 2597)
   Assured forwarding is used for signaling messages by default (AF31). It is less stringent than EF in a multiple dropping system. The AF values are containing two digits X and Y (AFXY), where X is describing the priority class and Y the drop level.
   Four classes X are reserved for AFXY: AF1Y (high priority), AF2Y, AF3Y and AF4Y (low priority).

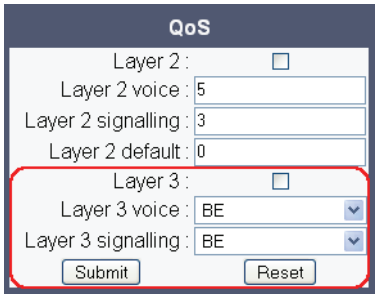
Three drop levels Y are reserved for AFXY: AFX1 (low drop probability), AFX2 and AFX3 (High drop probability). In the case of low drop level, packets are buffered over an extended period in the case of high drop level, packets are promptly rejected if they cannot be forwarded.

Data required

- **Layer 3**: Activates or deactivates QoS on layer 3.
  Value range: "Yes", "No".
  Default: "Yes".
- **Layer 3 voice**: Sets the CoS (Class of Service) value for voice data (RTP streams).
  Value range: "AF11", "AF12", "AF13", "AF21", "AF22", "AF23", "AF31", "AF32", "AF33", "AF41", "AF42", "AF43", "EF", "CST".
  Default: "EF".
- **Layer 3 signalling**: Sets the CoS (Class of Service) value for signaling.
  Value range: "AF11", "AF12", "AF13", "AF21", "AF22", "AF23", "AF31", "AF32", "AF33", "AF41", "AF42", "AF43", "EF", "CST").
  Default: "AF31".

Administration via WBM

Network > QoS



Administration via Local Phone

```
└── Administration
    └── Network
        └── QoS
            └── Service
                ├── Layer 3
                ├── Layer 3 voice
                └── Layer 3 signalling
```

3.3.2 Use DHCP

If this parameter is set to "Yes", the phone will search for a DHCP server on startup and try to obtain IP data and further configuration parameters from that central server.

If no DHCP server is available in the IP network, please deactivate this option. In this case, the IP address, subnet mask and default gateway/route must be defined manually.

The change will only have effect if you restart the phone.

The following parameters can be obtained by DHCP:

Basic informations

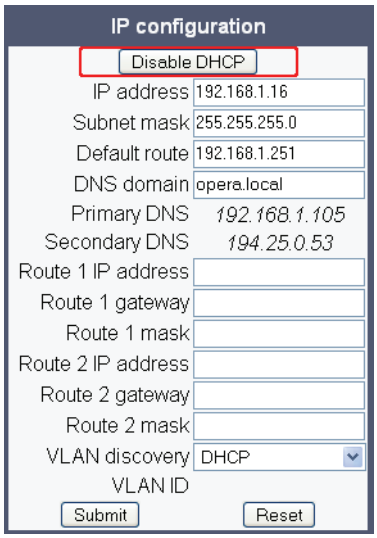
- IP Address
- Subnet Mask

Optional informations

- Default Route (Routers option 3)
- IP Routing/Route 1 & 2 (Static Routes option 33)
- SNTP IP Address (NTP Server option 42)
- Timezone offset (Time Server Offset option 2)
- Primary/Secondary IP Addresses (DNS Server option 6)
- DNS Domain Name (DNS Domain option 15)
- SIP Addresses / SIP Server & Registrar (SIP Server option 120)
- Vendor Unique (option 43)

Administration via WBM

Network > IP configuration



Administration via Local Phone

└── Administration
  └── Network
    └── IP Configuration
      └── **Use DHCP**

3.3.3 IP Address - Manual Configuration

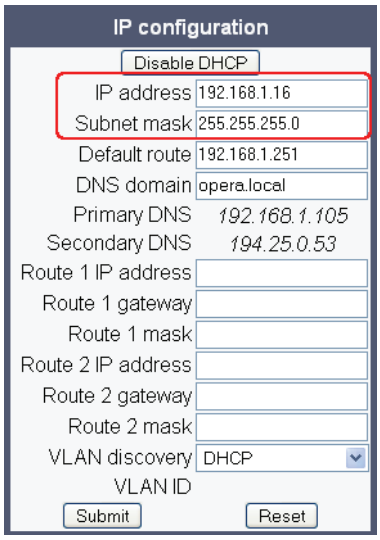
If not provided by DHCP dynamically, the phone's IP address and subnet mask must be specified manually.

Data required

- **IP address**: used for addressing the phone.
- **Subnet mask**: subnet mask that is needed for the subnet in use.

Administration via WBM

Network > IP configuration



Administration via Local Phone

```
└--- Administration
     └--- Network
          └--- IP Configuration
               |--- IP address
               └--- Subnet mask
```

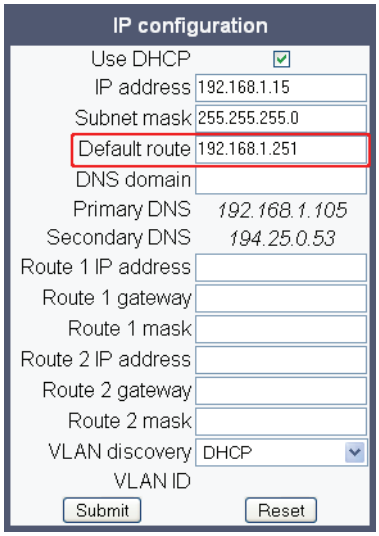
3.3.4 Default Route/Gateway

If not provided by DHCP dynamically (see Section 3.3.2, “Use DHCP”), enter the IP address of the router that links your IP network to other networks. If the value was assigned by DHCP, it can only be read.

The change will only have effect if you restart the phone.

Administration via WBM

Network > IP configuration



Administration via Local Phone

└── Administration
  └── Network
    └── IP Configuration
      └── **Route (default)**

3.3.5 Specific IP Routing

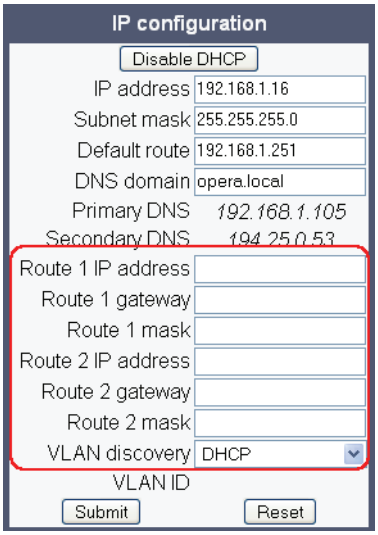
To have constant access to network subscribers of other domains, you can enter a total of two more network destinations, in addition to the default route/gateway. This is useful if the LAN has more than one router or if the LAN is divided into subnets.

Data required

- **Route 1/2 IP address**: IP address of the selected route.
- **Route 1/2 gateway**: IP address of the gateway for the selected route.
- **Route 1/2 mask**: Network mask for the selected route.

Administration via WBM

Network > IP configuration



Administration via Local Phone

```
└--- Administration
     └--- Network
          └--- IP Configuration
               |--- Route 1 IP
               |--- Route 1 gateway
               |--- Route 1 mask
               |--- Route 2 IP
               |--- Route 2 gateway
               └--- Route 2 mask
```

3.3.6 DNS

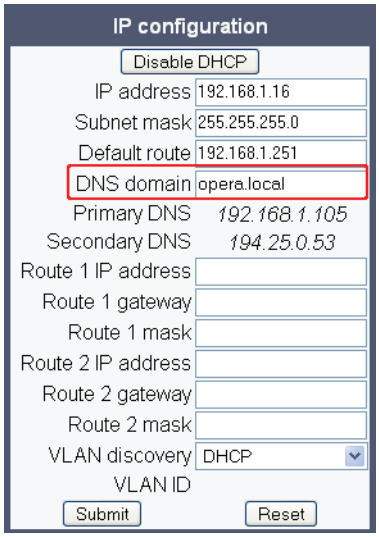
The main task of the domain name system (DNS) is to translate domain names to IP addresses. For some features and functions of the OpenStage phone, it is necessary to configure the DNS domain the phone belongs to, as well as the nameservers needed for DNS resolving.

3.3.6.1 DNS Domain Name

This is the name of the phone's local domain.

Administration via WBM

Network > IP configuration



Administration via Local Phone

└--- Administration
  └--- Network
    └--- IP Configuration
      └--- **DNS domain**

3.3.6.2 DNS Servers

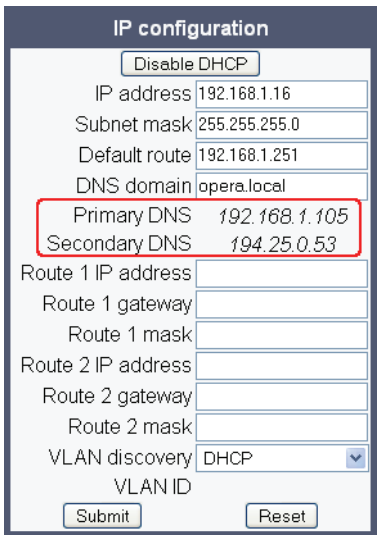
If not provided by DHCP automatically, a primary and a secondary DNS server can be configured.

Data required

- **Primary DNS**: IP address of the primary DNS server.
- **Secondary DNS**: IP address of the secondary DNS server.

Administration via WBM

Network > IP configuration



Administration via Local Phone

```
└--- Administration
     └--- Network
          └--- IP Configuration
               |--- Primary DNS
               └--- Secondary DNS
```

3.3.7 Configuration & Update Service (DLS)

The Deployment Service (DLS) is a HiPath Management application for administering workpoints in both HiPath and non-HiPath networks. Amongst the most important features are: security (e.g. PSS generation and distribution within an SRTP security domain), mobility for optiPoint and OpenStage SIP phones, software deployment, plug&play support, as well as error and activity logging.

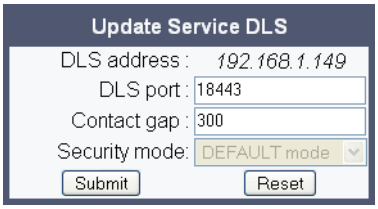
DLS address, i.e. the IP address or hostname of the DLS server, and **DLS port**, i.e. the port on which the DLS server is listening, are required to enable proper communication between phone and DLS. The **Contact gap** parameter controls a security function. It specifies a minimum time interval that must elapse between HTTP requests; any requests coming within that time will be ignored. The purpose is to prevent DoS (Denial of Service) attacks on the phone. The **Security mode** determines whether the communication between the phone and the DLS is secure. A secure connection is established by exchanging credentials between the DLS and the phone for mutual authentication. After this, the communication is encrypted, and a different port is used.

Data required

- **DLS address**: IP address or hostname of the server on which the Deployment Service is running.
- **DLS port**: Port on which the DLS Deployment Service is listening.
  Default: 18443.
- **Contact gap**: Minimum time interval in seconds that must elapse between HTTP requests, in order to prevent DoS attacks.
  Default: 300.
- **Security mode** / **Security status**: Determines whether the communication between the phone and the DLS is secure.
  Value range: "Default mode", "Secure mode".
  Default: "Default".

Administration via WBM

Network > Update Service (DLS)



Administration via Local Phone

```
└── Administration
    └── Network
        └── Update Service (DLS)
            ├── DLS address
            ├── DLS port
            ├── Contact gap
            └── Security status
```

3.3.8 SNMP

The Simple Network Management Protocol is used by network management systems for monitoring network-attached devices for conditions that warrant administrative attention. An SNMP manager surveys and, if needed, configures several SNMP elements, e.g. VoIP phones.

The OpenStage phone supports SNMP version 1 and 2.

There are currently 4 categories of trap that can be sent by the phones:

Standard SNMP traps

OpenStage phones support the following types of standard SNMP traps, as defined in RFC 1157:

- **coldStart**: sent if the phone does a full restart.
- **warmStart**: sent if only the phone software is restarted.
- **linkUp**: sent when IP connectivity is restored.

QoS Related traps

These traps are designed specifically for receipt and interpretation by the QDC collection system. The traps are common to SIP phones, HFA phones, Gateways, etc.

Traps for important high level SIP related problems

Currently, these traps are related to problems in registering with a SIP Server and to a failure in remotely logging off a mobile user. These traps are aimed at a non-expert user (e.g. a standard Network Management System) to highlight important telephony related problems.

Traps specific to OpenStage phones

Currently, the following traps are defined:

TraceEventFatal: sent if severe trace events occur; aimed at expert users.

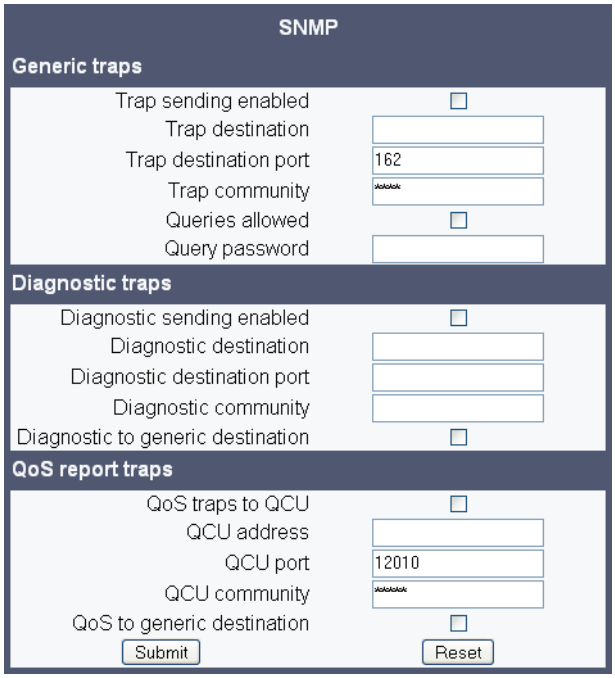
TraceEventError: sent if severe trace events occur; aimed at expert users.

Data required

- **Trap sending enabled**: Enables or disables the sending of a TRAP message to the SNMP manager.
  Value range: "Yes", "No".
  Default: "No".
- **Trap destination**: IP address or hostname of the SNMP manager that receives traps.
- **Trap destination port**: Port on which the SNMP manager is receiving TRAP messages.
- Default: 162.
- **Trap community**: SNMP community string for the SNMP manager receiving TRAP messages.
  Default: "snmp".
- **Queries allowed**: Enables or disables queries from the SNMP manager.
- **Query password**: Password for the execution of a query by the SNMP manager.
- **Diagnostic sending enabled**: Enables or disables the sending of diagnostic data to the SNMP manager.
  Value range: "Yes", "No".
  Default: "No".
- **Diagnostic destination**: IP address or hostname of the SNMP manager receiving diagnostic data.
- **Diagnostic destination port**: Port on which the SNMP manager is receiving diagnostic data.
- **Diagnostic community**: SNMP community string for the SNMP manager receiving diagnostic data.
- **QoS traps to QCU**: Enables or disables the sending of TRAP messages to the QCU server.
  Value range: "Yes", "No".
  Default: "No".
- **QCU address**: IP address of the QCU server.
- **QCU port**: Port on which the QCU server is listening for messages.
  Default: 12010.
- **QCU community**: QCU community string.
  Default: "QOSCD".
- **QoS to generic destination / QoS to generic device**: Enables or disables the sending of QoS traps to a generic destination.
  Value range: "Yes", "No".
  Default: "No".

Administration via WBM

System > SNMP



Administration via Local Phone

```
└--- Administration
     └--- System
          └--- SNMP
               |--- Trap sending enabled
               |--- Trap destination
               |--- Trap destination port
               |--- Trap community
               |--- Diag sending enabled
               |--- Diag destination
               |--- Diag destination port
               |--- Diag community
               |--- QoS traps to QCU
               |--- QCU address
               |--- QCU port
               |--- QCU community
               └--- QoS to generic device
```

3.4 Speech Encryption (V1R4.x upwards)

With software version V1R4.x or higher, secure speech transmission via SRTP is possible.

If **Use secure calls** is activated, the encryption of outgoing calls is enabled, and the phone is capable of receiving encrypted calls. An icon in the call view tells the user whether a call is secure or not. If an active call changes from secure to insecure, e. g. after a transfer, a popup window and an alert tone will notify the user. For enabling secure calls, a TLS connection to the HiPath 8000 is required.

For secure calls, it is required that both endpoints support SRTP. The secure call indication tells the user that the other endpoint has acknowledged the secure connection.

In order to use SRTP, the phone must be configured for NTP (for further information please see Section 3.5.4, “Date and Time”). The reason is that the key generation (MIKEY) uses the system time of the particular device as a basis. Thus, encryption will only work correctly if all devices have the same UTC time.

If **SIP server certificate validation** resp. **Backup SIP server certificate validation** is activated, the phone will validate the server certificate sent by the HiPath 8000 in order to establish a TLS connection. The server certificate is validated against the root certificate from the trusted certificate authority (CA), which must be stored on the phone first. For delivering the root certificate, a DLS (Deployment Software) server is required.

Administration via WBM

System > Security

Administration via Local Phone

- Administration
  - System
    - Security
      - **Server cerfificate**
      - **Backup certificate**
      - **Use secure calls**

3.5 System Settings

3.5.1 Terminal and User Identity

3.5.1.1 Terminal Identity

Within a SIP environment, both Terminal Number and Terminal Name may serve as a phone number. The values are used in the userinfo part of SIP URIs.

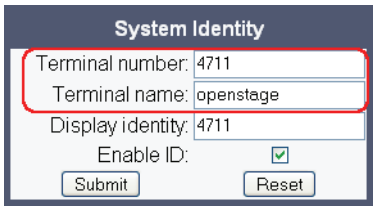
In order to register with a SIP registrar, the phone sends REGISTER messages to the registrar containing the contents of **Terminal number**

Data required

- **Terminal number**: Number to be registered at the SIP registrar.
- **Terminal name**: Name to be registered at the SIP registrar.

Administration via WBM

System > System Identity



Administration via Local Phone

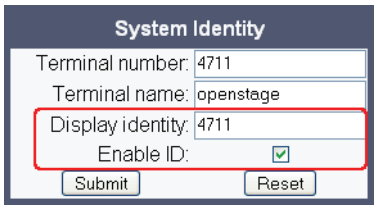
```
└--- Administration
     └--- System
          └--- Identity
               |--- Terminal number
               └--- Terminal name
```

3.5.1.2 Display Identity

If an individual name oder number is entered as **Display identity**, and **Enable ID** is activated, it is displayed in the phone's status bar instead of the Terminal number or Terminal name.

Administration via WBM

System > System Identity



Administration via Local Phone

```
└── Administration
    └── System
        └── Identity
            ├── Display identity
            └── Enable ID
```

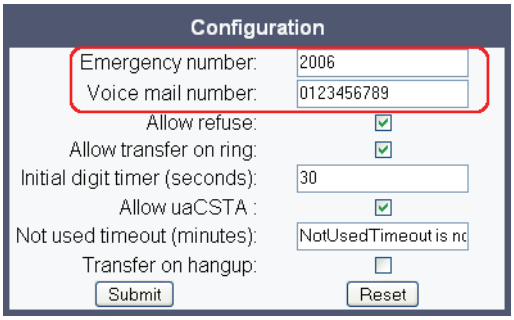
3.5.2 Emergency and Voice Mail

It is important to have an **Emergency number** configured. If the phone is locked, a clickable area for making an emergency call is created.

If a mailbox located at a remote server shall be used, its **Voice mail number** must be entered.

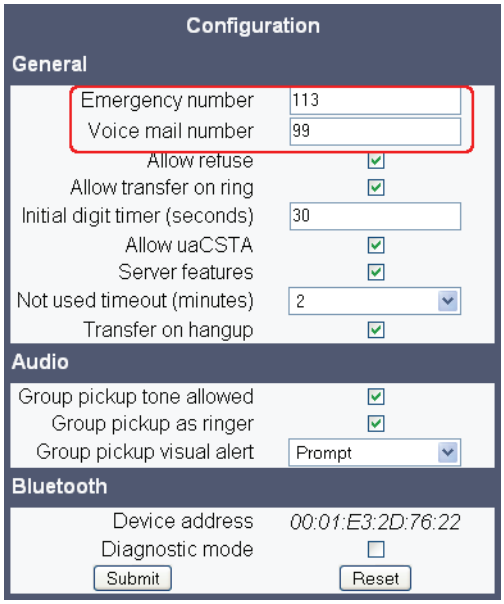
Administration via WBM (V1R2.x)

System > Features > Configuration



Administration via WBM (V1R3.x upwards)

System > Features > Configuration



Administration via Local Phone

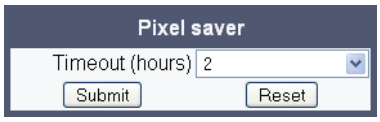
- Administration
  - System
    - Features
      - Configuration
        - General
          - **Emergency number**
          - **Voicemail number**

3.5.3 Pixel Saver (OpenStage 40/60/80)

After the phone has beeen incative within a specified timespan, the display backlight is switched off. The length of the timespan ranges from 2 hours to 8 hours.

Administration via WBM

Local functions > Pixel saver



Administration via Local Phone

- Administration
  - Local Functions
    - **Pixel saver**

3.5.4 Date and Time

If the DHCP server in your network provides information about the SNTP server access, the correct date and time is automatically shown on the phone. If the DHCP server in your network does not provide an SNTP address, you have to set the SNTP address manually, using the **SNTP IP address** parameter. If no SNTP server is available, you have to configure the date and time manually.

For correct display of the current time, the **Timezone offset** must be set appropriately. This is the time offset from UTC (Coordinated Universal Time). If, for instance, the phone is located in Munich, Germany, the offset is +1 (or simply 1); if it is located in Los Angeles, USA, the offset is -8. For countries or areas with half-our time zones, like South Australia or India, non-integer values can be used, for example 10.5 for South Australia (UTC +10:30).

If the phone is located in a country with daylight saving, the administrator can choose whether daylight saving time is activated manually or automatically. If **Daylight saving** is enabled, and **Auto time change** is disabled, daylight saving time (DST) is in effect immediately. If **Auto time change** is enabled, daylight saving is controlled by the **Time zone** parameter. This selects the daylight saving time zone which is characterized by the start and end date for daylight saving time.

The **Difference (minutes)** provides the time difference for daylight saving time in minutes. This parameter is required also when **Auto time change** is enabled. In Germany, for instance, as in most countries, this is +60.

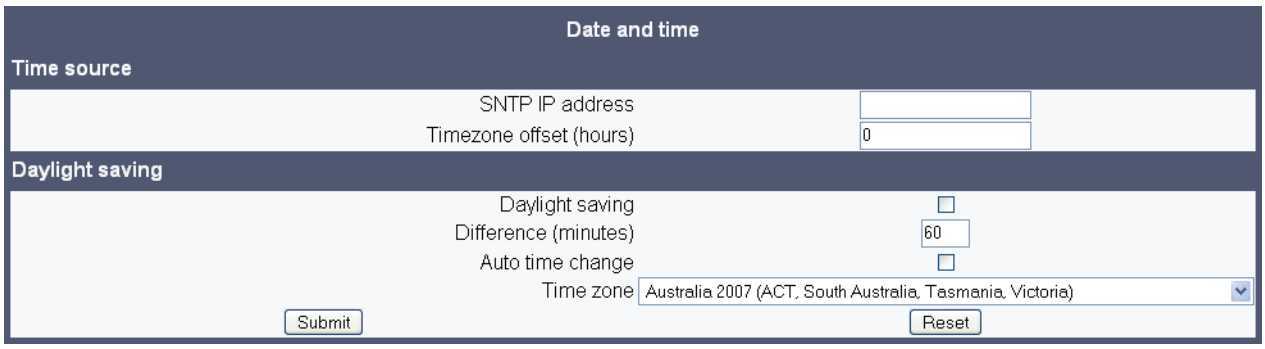
3.5.4.1 SNTP is available, but no automatic configuration by DHCP server

Data required

- **SNTP IP address**: IP address or hostname of the SNTP server.
- **Timezone offset (hours)**: Shift in hours corresponding to UTC.
- **Daylight saving**: Enables or disables daylight saving time in conjunction with **Auto time change**.
  Value range: "Yes", "No".
- **Difference (minutes)**: Time difference when daylight saving time is in effect.
- **Auto time change** / **Auto DST**: Enables or disables automatic control of daylight saving time according to the **Time zone**.
  Value range: "Yes", "No".
- **Time zone** / **DST zone**: Area with common start and end date for daylight saving time.
  Value range: "Australia 2007 (ACT, South Australia, Tasmania, Victoria)", "Australia 2007 (New South Wales)", "Australia (Western Australia)", "Australia 2008+ (ACT, New South Wales, South Australia, Tasmania, Victoria)", "Brazil", "Canada", "Canada (Newfoundland)", "Europe (Portugal, United Kingdom)", "Europe (Finland)", "Europe (Rest)", "Mexico", "United States".

Administration via WBM

Date and Time



Administration via Local Phone

```
└--- Administration
     └--- Date and Time
          |--- SNTP IP address
          └--- Timezone offset
```

3.5.4.2 No SNTP server available

If no SNTP server is available, date and time must be set manually.

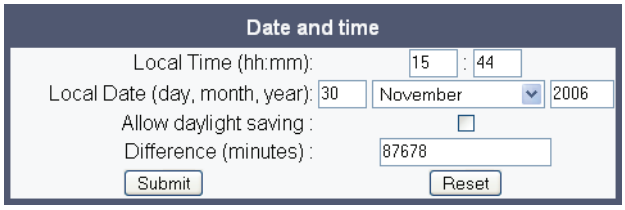
> The manual setting of Time and Date is located in the user menu, not in the administrator menu.

Data required

- **Local time (hh:mm)**: Local time.
- **Local date (day, month, year)**: Local date.
- **Allow daylight saving**: Defines whether there is daylight is set.
- **Difference (minutes)**: Timezone offset in minutes.

Administration via WBM

(User pages >) Date and time



Administration via Local Phone

└--- Menu
  └--- Date and Time
    |--- **Time**
    |--- **Date**
    |--- **Daylight saving**
    └--- **Difference (mins)**

3.5.5 SIP Addresses and Ports

3.5.5.1 SIP Addresses

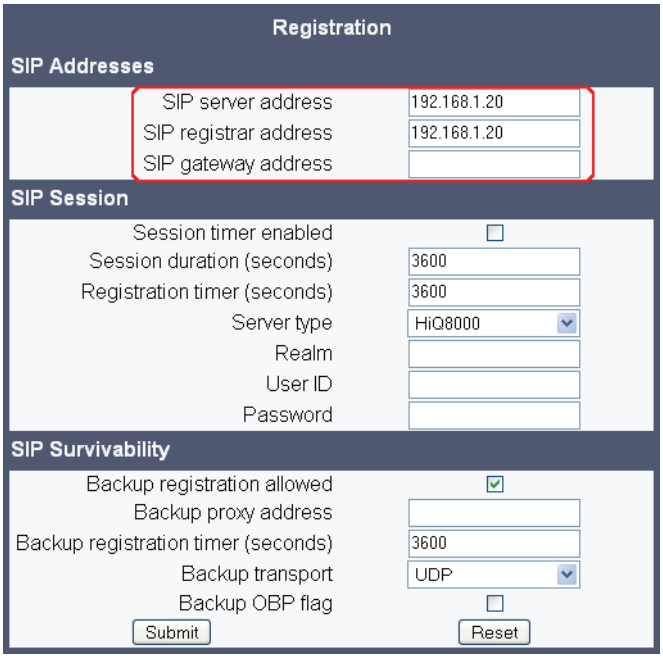
In this group of parameters, the IP addresses or host names for the SIP server, the SIP registrar, and the SIP gateway are defined.

SIP server address provides the IP address or host name of the SIP proxy server (Hipath 8000). This is necessary for outgoing calls. **SIP registrar address** contains the IP address or host name of the registration server, to which the phone will send REGISTER messages. When registered, the phone is ready to receive incoming calls. **SIP gateway address** gives the IP address or host name of the SIP gateway. The SIP gateway performs a conversion of SIP to TDM, which enables to phone directly into the public network.**Data required**

- **SIP server address**: IP address or host name of the SIP proxy server.
- **SIP registrar address**: IP address or host name of the registration server.
- **SIP gateway address**: IP address or host name of the SIP gateway.

Administration via WBM

System > Registration



Administration via Local Phone

```
└--- Administration
     └--- System
          └--- Registration
               └--- SIP Addresses
                    ├--- SIP server
                    ├--- SIP registrar
                    └--- SIP gateway
```

3.5.5.2 SIP Ports

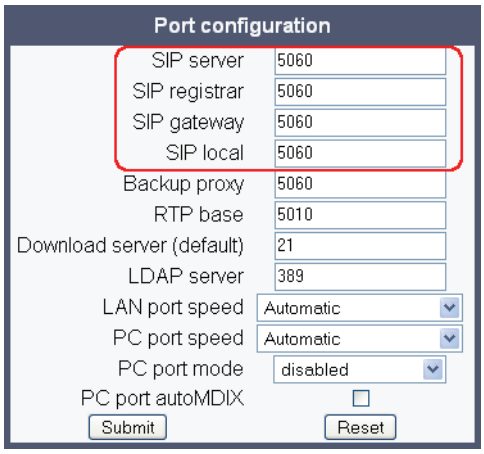
In this group of parameters, the ports for the SIP server, the SIP registrar, and the SIP gateway are defined (for further information see Section 3.5.5.1, “SIP Addresses”), as well as the SIP port used by the phone (**SIP local**).

Data required

- **SIP server**: Port of the SIP proxy server.
  Default: 5060.
- **SIP registrar**: Port of the server at which the phone registers.
  Default: 5060.
- **SIP gateway**: Port of the SIP gateway.
  Default: 5060.
- **SIP local**: Port used by the phone for sending and receiving SIP messages.
  Default: 5060.

Administration via WBM

Network > Port configuration



Administration via Local Phone

└--- Administration
  └--- Network
    └--- Port Configuration
      |--- **SIP server**
      |--- **SIP registrar**
      |--- **SIP gateway**
      └--- **SIP local**

3.5.6 SIP Registration

Registration is the process by which centralized SIP Server/Registrars become aware of the existence and readiness of an endpoint to make and receive calls. The phone supports a number of configuration parameters to allow this to happen. Registration can be authenticated or un-authenticated depending on how the server and phone is configured.

Unauthenticated Registration

For unauthenticated registration, the following parameters must be set on the phone: Terminal number or Terminal name (see Section 3.5.1.1, “Terminal Identity”), SIP server and SIP registrar address (see Section 3.5.5.1, “SIP Addresses”). Moreover, the correct **Server type** must be set. Additionally, the expiry time of a registration can be specified by **Registration timer**.

In unauthenticated mode, the server must pre-authenticate the user. This procedure is server specific and is not described here.

Authenticated Registration

The phone supports the digest authentication scheme and requires some parameters to be configured in addition to those for unauthenticated registration. By providing a **User ID** and a **Password** which match with a corresponding account on the SIP registrar, the phone authenticates itself. Optionally, a **Realm** can be added. This parameter specifies the protection domain wherein the SIP authentication is meaningful. The protection domain is globally unique, so that each protection domain has its own arbitrary usernames and passwords.

A challenge from the server for authentication information is not only restricted to the REGISTER message, but can also occur in response to other SIP messages, e. g. INVITE.

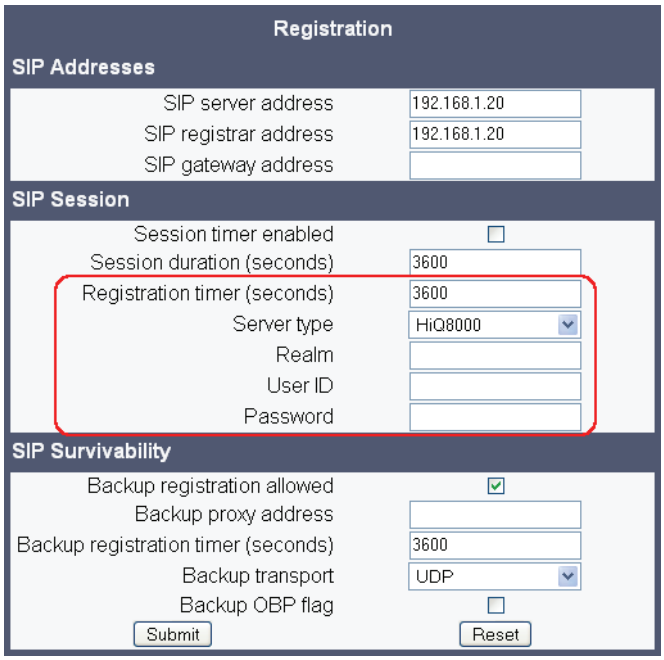
If registration has not succeeded at startup or registration fails after having been previously successfully registered the phone will try to re-register every 30 seconds. This is not configurable.

Data required

- **Registration timer (seconds)**: Expiry time of the registration in seconds.
  Default value: 3600.
- **Server type**: Type of server the phone will register to.
  Value range: "Other", "HiQ8000".
  Default value: "HiQ8000".
- **Realm**: Protection domain for authentication.
- **User ID**: Username required for an authenticated registration.
- **Password**: Password required for an authenticated registration.

Administration via WBM

System > Registration



Administration via Local Phone

└--- Administration
  └--- System
    └--- Registration
      └--- SIP Session
        |--- **Registration timer**
        |--- **Server type**
        |--- **Realm**
        |--- **User ID**
        └--- **Password**

3.5.7 SIP Connection and Communication

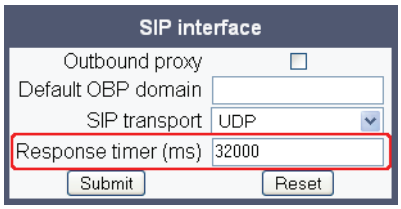
3.5.7.1 Response Timer

The **Response timer** is started whenever the phone sends a new message to the SIP server. If the timer expires before the phone gets a response from the SIP server, the phone assumes that the server had died and then attempts to contact the backup server, if configured. If there is no backup server configured, the phone just tidies up internally.

The data is given in milliseconds. The default value is 32 000; for the HiPath 8000, the recommended setting is 3.7 seconds (3700 ms).

Administration via WBM

System > SIP interface



Administration via Local Phone

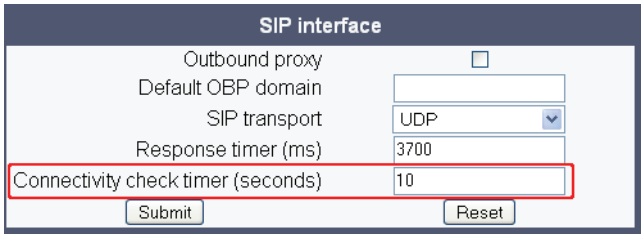
└── Administration
  └── System
    └── SIP Interface
      └── **Response timer (ms)**

3.5.7.2 Connectivity Check

A regular check ensures that the TLS link is active. When the **Connectivity check timer** is set to a non-zero value, test messages will be sent at the defined interval. If the link is found to be dead, the phone searches for another links.

Administration via WBM

System > SIP interface



3.5.7.3 Outbound Proxy

If this option set to "Yes", the phone routes outbond requests to the configured proxy, i. e. the SIP server/registrar. The outbound proxy will fulfill the task of resolving the domain contained in the SIP request. If "No" is set, the phone will attempt to resolve the domain by itself.

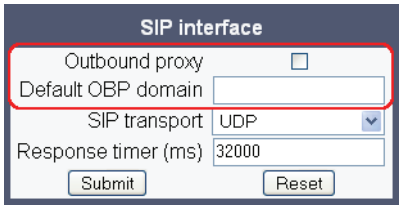
If a **Default OBP** (Outbound Proxy) **domain** is set and the number or name dialed by the user does not provide a domain, this value will be appended to the name or number. Otherwise, the domain of the outbound proxy will be appended.

Data required

- **Outbound proxy**: Determines whether an outbound proxy is used or not.
  Value range: "Yes", "No".
  Default: "No".
- **Default OBP domain**: Alternative value for the domain that is given in the outbound request.

Administration via WBM

System > SIP interface



Administration via Local Phone

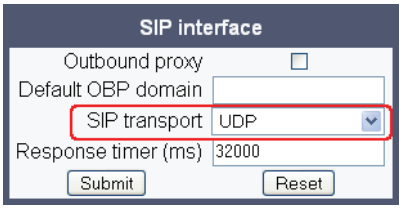
```
└--- Administration
     └--- System
          └--- SIP Interface
               ├--- Outbound proxy
               └--- Default OBP domain
```

3.5.7.4 SIP Transport Protocol

Selects the transport protocol to be used for SIP messages. The values "UDP", "TCP", and "TLS" are available. The default is "UDP".

Administration via WBM

System > SIP interface



Administration via Local Phone

└--- Administration
  └--- System
    └--- SIP Interface
      └--- **SIP transport**

3.5.8 SIP Session Timer

Session timers provide a basic keep-alive mechanism between 2 user agents or phones. This mechanism can be useful to the endpoints concerned or for stateful proxies to determine that a session is still alive. This is achieved by the phone sending periodic re-INVITEs to keep the session alive. If no re-INVITE is received before the interval passes, the session is considered terminated. Both phones are supposed to terminate the call, and stateful proxies can remove any state for the call.

This feature is sufficiently backward compatible such that only one end of a call needs to implement the SIP extension for it to work.

The parameter **Session timer enabled** determines whether the mechanism shall be used, and **Session duration (seconds)** sets the expiration time, and thus the interval between refresh re-INVITEs.

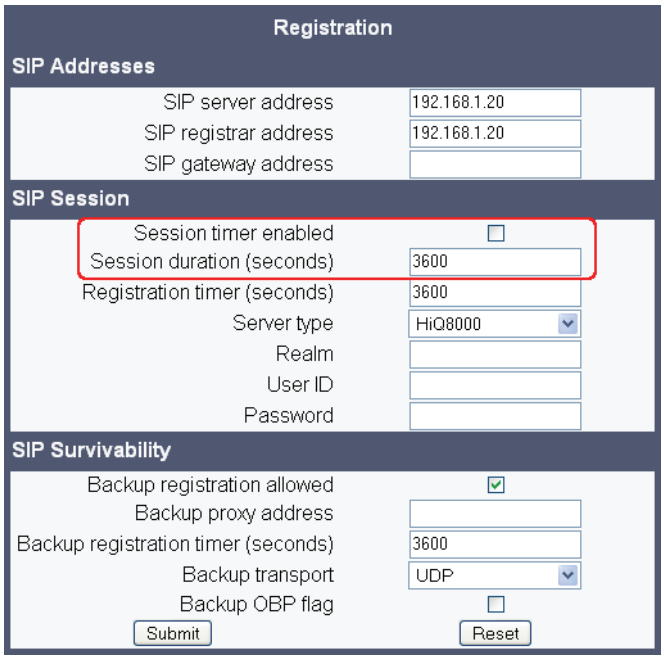
Some server environments support their own mechanism for auditing the health of a session (e. g. Broadsoft). In these cases, the **Session timer** must be deactivated.

Data required

- **Session timer enabled**: Activates or deactivates the session timer mechanism.
  Value range: "Yes", "No".
  Default value: "No".
- **Session duration (seconds)**: Sets the expiration time for a SIP session.
  Default: 3600.

Administration via WBM

System > Registration



Administration via Local Phone

```
└── Administration
    └── System
        └── Registration
            └── SIP session
                ├── Session timer
                └── Session duration
```

3.5.9 SIP Survivability

The survivability feature will allow the SIP User Agent to register with a backup SIP proxy which will be used to make and receive calls when the primary SIP proxy fails or is not reachable due to a network failure.

The prime reason for this feature is to maintain basic call functionality when network failures occur, and it is therefore expected that some features and functionality will not be available when working in survivability mode.

The **Backup registration flag** indicates whether or not the phone treats the backup proxy server as a SIP registrar. If set to "Yes", the phone tries to register its SIP address with the server whose IP address or hostname is specified by **Backup proxy address**.

The **Backup registration timer** determines the duration of a registration with the SIP server.

The **Backup transport** option displays the current transport protocol used to carry SIP messages to the Backup proxy server.

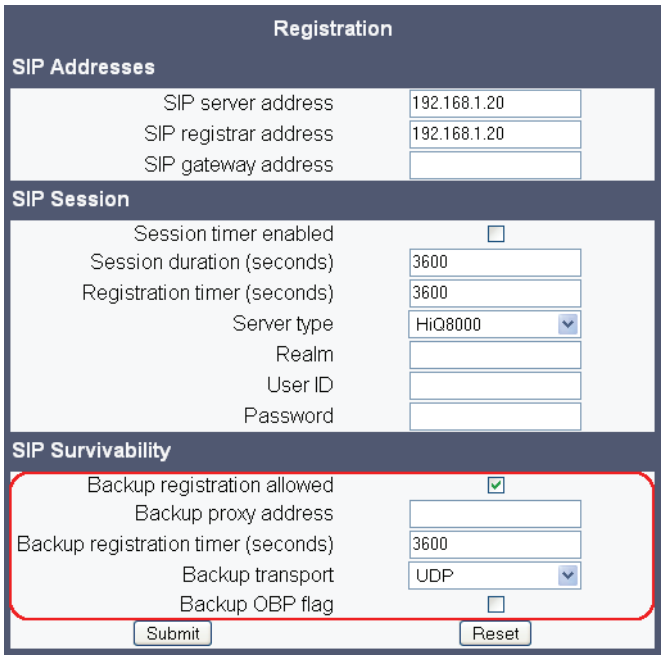
The **Backup OBP flag** indicates whether or not the Backup proxy server is used as an outbound proxy.

Data required

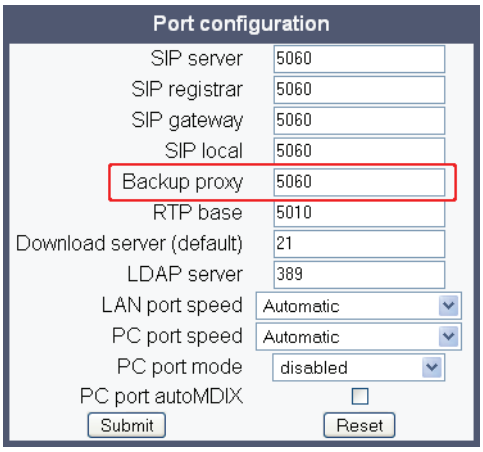
- **Backup registration flag**: Determines whether or not the backup proxy is used as a SIP Registrar.
  Value Range: "Yes", "No".
  Default: "Yes".
- **Backup proxy address**: IP address or hostname of the backup proxy server.
- **Backup registration timer**: Expiry time of the registration in seconds.
  Default: 3600.
- **Backup transport**: Transport protocol to be used for messages to the backup proxy.
  Value range: "TCP", "UDP", "TLS".
  Default: "UDP".
- **Backup OBP flag**: Determines whether or not the backup proxy is used as an outbound proxy.
  Value range: "Yes", "No".
  Default: "No".
- Network > Port Configuration > **Backup proxy**: Port of the backup proxy server.
  Default: 5060.

Administration via WBM

System > Registration



Network > Port configuration



Administration via Local Phone

- Administration
  - System
    - Registration
      - SIP Session
      - SIP Survivability
        - **Backup registration flag**
        - **Backup proxy address**
        - **Backup transport**
        - **OBP flag**

- Administration
  - Network
    - Port Configuration
      - **Backup proxy**

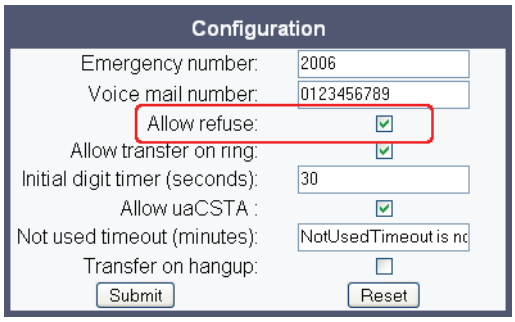
3.6 Features - Configuration

3.6.1 Allow Refuse

This parameter defines whether the Refuse Call feature is available on the phone. The possible values are "Yes" or "No". The default is "Yes".

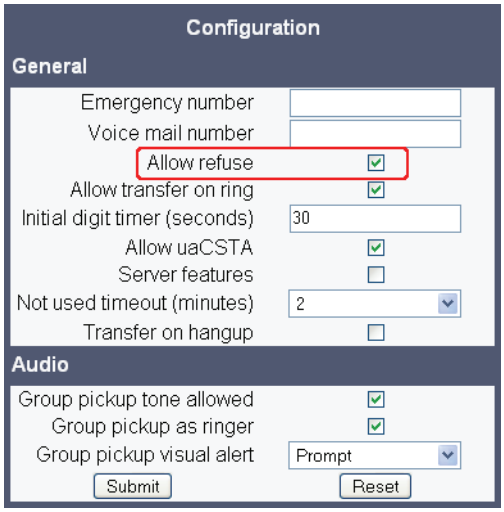
Administration via WBM (V1R2.x)

System > Features > Configuration



Administration via WBM (V1R3.x upwards)

System > Features > Configuration



Administration via Local Phone

- Administration
  - System
    - Features
      - Configuration
        - General
          - **Allow refuse**

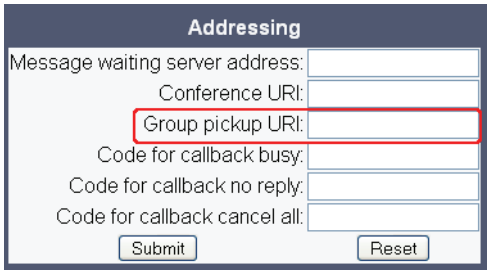
3.6.2 Group Pickup

3.6.2.1 Feature Code

This feature allows a user to collect a call from any ringing phone that is in the same pickup group. To be a member of a Call Pickup group, the phone must be configured with the corresponding URI of the Call Pickup group service provided by the server. This URI has the following form: <groupcallpickup>@<SIP Server IP> (for instance **3@172.16.127.95 or Domain Name).

Administration via WBM

System > Features > Addressing



Administration via Local Phone

└--- Administration
  └--- System
    └--- Features
      └--- Addressing
        └--- **Group pickup URI**

3.6.2.2 Pickup alert (V1R3.x upwards)

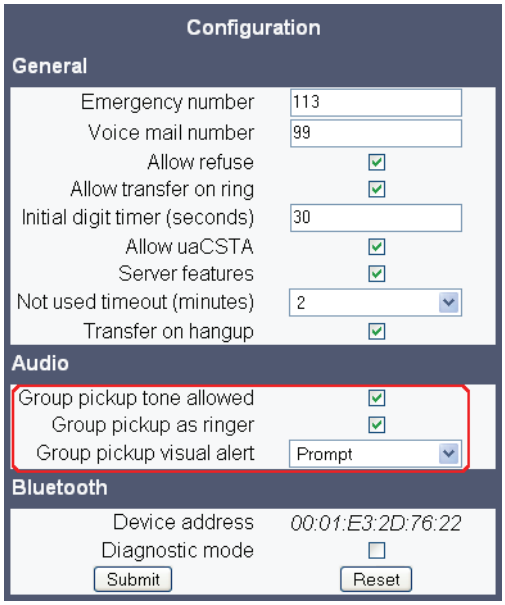
If desired, an incoming call for the pickup group can be indicated acoustically.

The **Group pickup tone allowed** parameter activates or deactivates the generation of an acoustic signal for incoming pickup group calls. The default is "Yes". If this is activated, **Group pickup as ringer** determines whether the current ringtone or an alert beep is used. If set to "Yes", a pickup group call will be signaled by a short standard ringtone. If set to "No", a pickup group call will be signaled by an alert tone. The default is "Yes".

Group pickup visual alert defines the user action required to accept a pickup call. If "Prompt" is selected, an incoming pickup call is signaled by an alert on the phone GUI. As soon as the user goes off-hook or presses the speaker key, the pickup call is accepted. Alternatively, the user can press the corresponding function key, if configured. If "Notify" is selected, an incoming pickup call is signaled by an alert on the phone GUI. To accept the call, the user must confirm the alert or press the corresponding function key, if configured.

Administration via WBM

System > Features > Configuration



Administration via Local Phone

- Administration
  - System
    - Features
      - Configuration
        - Audio
          - **Group pickup tone allowed**
          - **Group pickup as ringer**
          - **Group pickup visual alert**

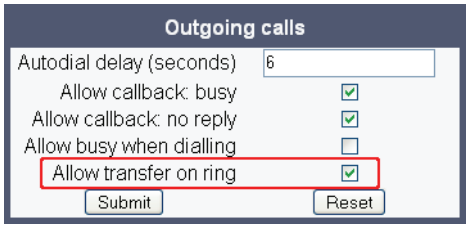
3.6.3 Call Transfer

3.6.3.1 Transfer on Ring

If this function is active, a call can be transferred after the user has dialled the third participant's number, but before the third party has answered the call. This feature is enabled or disabled in the User menu. The default is "Yes".

Administration via WBM

(User) Configuration > Outgoing calls



Administration via Local Phone

```
|--- User
     |--- Configuration
          |--- Outgoing calls
               |--- Transfer on ring
```

3.6.3.2 Transfer on Hangup

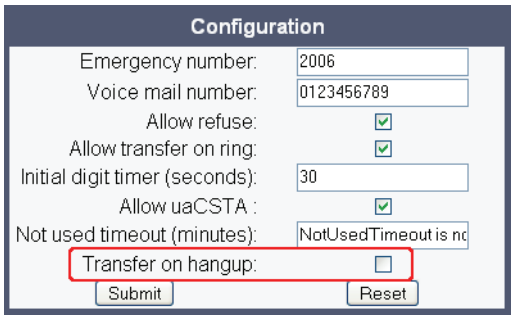
This feature applies to the following scenario: While A is talking to B, C calls A. A accepts the call, so B is on hold and the call between A and C is active. If **Transfer on hangup** is enabled, and A goes on-hook, B gets connected to C.

If Transfer on hangup is disabled, C will be released when A hangs up, and A has the possibility to reconnect to B.

The default is "No".

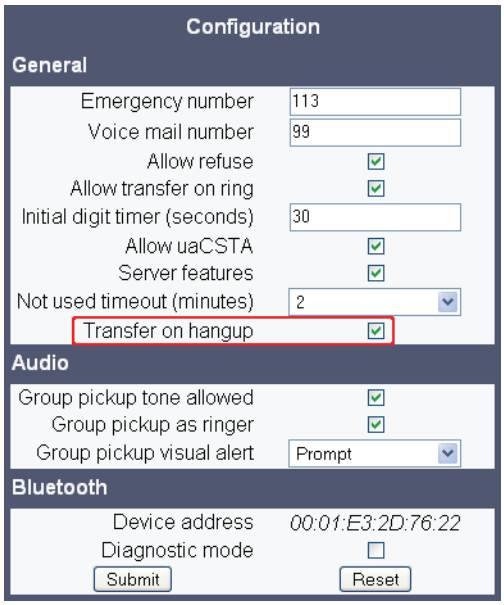
Administration via WBM (V1R2.x)

System > Features > Configuration



Administration via WBM (V1R3.x upwards)

System > Features > Configuration



Administration via Local Phone

```
|--- Administration
     |--- System
          |--- Features
               |--- Configuration
                    |--- General
                         |--- Transfer on hangup
```

3.6.4 Callback URIs

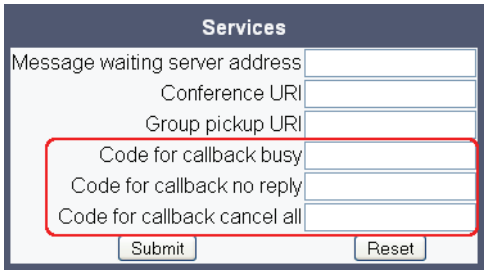
The Callback option allows the user to request a callback on certain conditions. The callback request is sent to the SIP server. The **Code for callback busy** requests a callback if the line is busy, i. e. if there is a conversation on the remote phone. **Code for callback no reply** applies when the call is not answered, i. e. if nobody lifts the handset or accepts the call in another way. The **Code for callback cancel all** all deletes all the callback requests stored previously on the telephone system/SIP server.

Data required

- **Code for callback busy** / **Callback: Busy**: Access code that is sent to the server if the line is busy.
- **Code for callback no reply** / **Callback: No reply**: Access code that is sent to the server if the callee does not reply.
- **Code for callback cancel all** / **Callback: Cancel all**: Access code for canceling all call-back requests on the server.

Administration via WBM

System > Features > Services



Administration via Local Phone

```
└--- Administration
     └--- System
          └--- Features
               └--- Addressing
                    |--- Callback: Busy
                    |--- Callback: No reply
                    └--- Callback: Cancel all
```

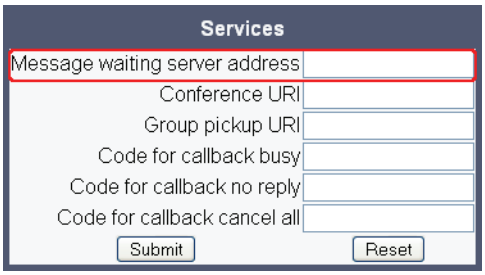
3.6.5 Message Waiting Address

The MWI (Message Waiting Indicator) is an optical signal which indicates that voicemail messages are on the server. Depending on the SIP server / gateway in use, the **Message waiting server address**, that is the address or host name of the server that sends message waiting notifications to the phone, must be configured.

With HiPath 8000, this setting is not typically necessary for enabling MWI functionality.

Administration via WBM

System > Features > Services



Administration via Local Phone

└--- Administration
  └--- System
    └--- Features
      └--- Addressing
        └--- **MWI server URI**

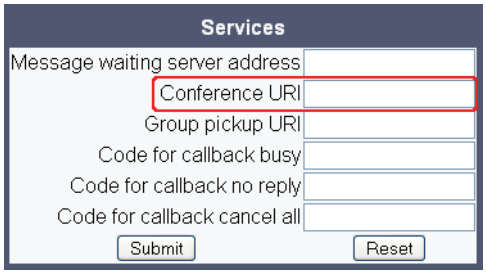
3.6.6 System Based Conference

The **Conference URI** provides the number/URI used for system based conferences, which can involve more than three members. This feature is not available with every system.

It is recommended not to enter the full URI, but only the user part. For instance, enter "123", not "123@<SIP SERVER ADDRESS>". A full address in this place might cause a conflict when the HiPath 8000 uses multiple nodes.

Administration via WBM

System > Features > Services

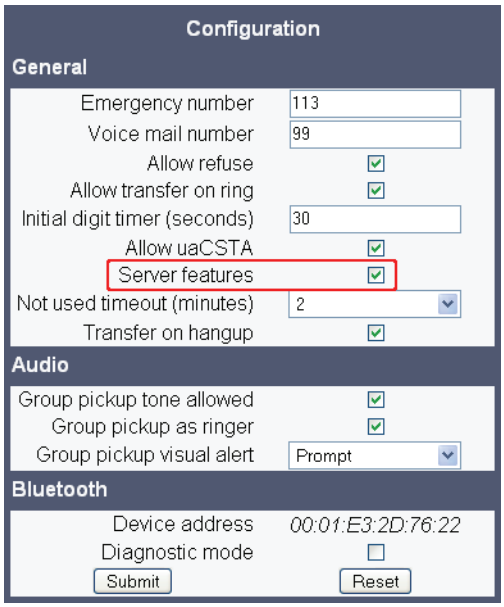


3.6.7 Server Based Features (V1R3.x upwards)

The use of several server based features, such as server based DND (Do Not Disturb) and server based call forwarding, is enabled or disabled here.

Administration via WBM

System > Features > Configuration



Administration via Local Phone

└--- Administration
└--- System
└--- Features
└--- Configuration
└--- General
└--- **Server features**

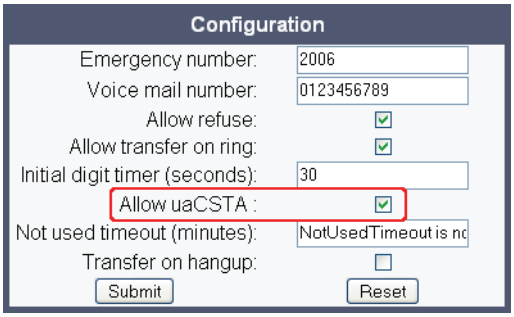
3.6.8 uaCSTA Interface

User Agent CSTA (uaCSTA) is a limited subset of the CSTA protocol, which allows external CTI applications to interact with the phone.

If **Allow uaCSTA** is enabled, applications which support the uaCSTA standard will have access to the OpenStage phone. The default is "Yes".

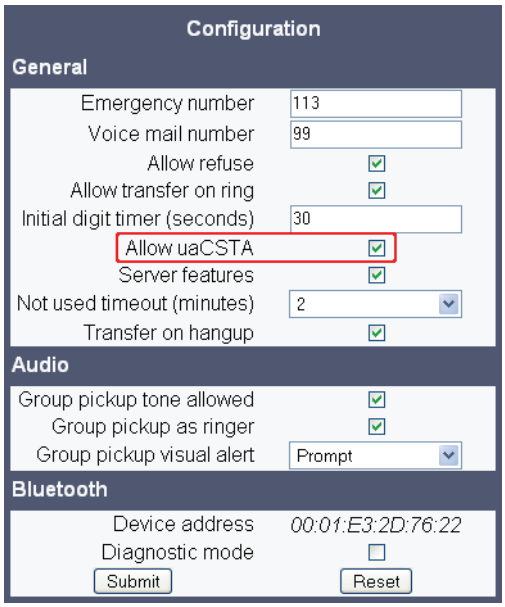
Administration via WBM (V1R2.x)

System > Features > Configuration



Administration via WBM (V1R3.x upwards)

System > Features > Configuration



Administration via Local Phone

- Administration
  - System
    - Features
      - Configuration
        - General
          - **Allow uaCSTA**

3.6.9 Local Menu Timeout

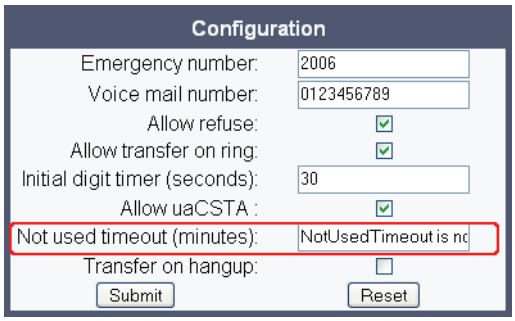
The timeout for the local user and admin menu is configurable. When the time interval is over, the menu is closed and the administrator/user is logged out.

The timeout may be helpful in case a user does a long press on a line key unintentionally, and thereby invokes the key configuration menu. The menu will close after the timeout, and the key will return to normal line key operation.

The timeout ranges from 1 to 5 five minutes. The default value is 2.

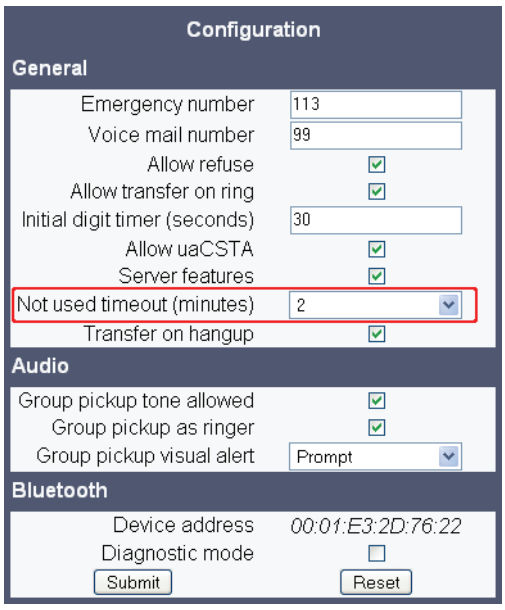
Administration via WBM (V1R2.x)

System > Features > Configuration



Administration via WBM (V1R3.x upwards)

System > Features > Configuration



Administration via Local Phone

└--- Administration
  └--- System
    └--- Features
      └--- Configuration
        └--- General
          └--- **Not used timeout**

3.7 Multiline Appearance/Keyset

This feature is available only on OpenStage 40 and OpenStage 60/80 phones.

A phone that has more than one line associated to it, and therefore works as a multiline phone, is referred to as "keyset". The lines are assigned to the phone by setting up a separate line key for each line.

The multiline appearance feature allows for multiple lines to be assigned to a keyset and for a line to be assigned to multiple keysets. This feature requires configuration in the HiPath 8000 and in the telephone, and is particularly useful for executive-assistant arrangements.

For each keyset, a primary line is required. The primary line is the dialing number for that keyset.

There are two types of line:

- **Private line**: A line that appears on only one keyset.
- **Shared line**: A line that is shared between keysets.

3.7.1 Line key configuration

A line corresponds to a SIP address of record (AoR), which can have a form similar to an E-mail address, or can be a phone number. It is defined by the **Address of record** parameter. For registration of the line, a corresponding entry must exist on the SIP server resp. the SIP registrar server.

A label can be assigned to the line key by setting its **Key label**.

Every keyset must necessarily have a line key for the primary line. To configure the key of the primary line, set **Primary line** to "true".

If **Ring on/off** is checked, the line will ring when an incoming call occurs, and a popup will appear on the display. If the option is not checked, the incoming call will be indicated only by the blinking of the key's LED. If it is desired that the line ring with a delay, the time interval in seconds can be configured by **Ring delay**.

When the user lifts the handset in order to initiate a call, the line to be used is determined by selection rules. To each line, a priority is assigned by the **Selection order** parameter. A line with the rank 1 is the first line to be considered for use. If more than one lines have the same rank, the selection is made according to the key number. Note that Selection order is a mandatory setting; it is also used in the Terminating line preference, as well as in other functions.

The **Address** (Address of Record) parameter gives is the phone number resp. SIP name corresponding to the entry in the SIP registrar at which the line is to be registered.

For the configuration of line keys, the use of the DLS (Deployment Service) is recommended. For operating the DLS, please refer to the DLS user's guide. Alternatively, the web interface or the local menu can be used. Note that the creation of a new line key and the configuration of some parameters can not be accomplished by the phone's local menu.
Generally, it is advisable to restrict the user's possibilities to modify line keys. This can be achieved solely by the DLS. For further instructions, see the DLS Administration Guide.

The **Realm**, a protection domain used for authenticated access to the SIP server, works as a name space. Any combination of user id and password is meaningful only within the realm it is assigned to. The other parameters necessary for authenticated access are **User Identifier** and **Password**. For all three parameters, there must be corresponding entries on the SIP server.

The **Shared type** parameter determines whether the line is a shared line, i. e. shared with other endpoints, or a private line, i .e. available exclusively for this endpoint. A line that is configured as primary line on one phone can be configured as secondary line on other phones.

When **Allow in Overview** is set to "Yes", the line will be visible in the line overview on the phone's display.

Data required

- **Key label <n>**: Set the label of the line key with the key number <n>.
  Default: "Line".
- **Primary line**: Determines whether the line is the primary line.
  Value range: "Yes", "No".
  Default: "No".
- **Ring on/off**: Determines whether the line rings on an incoming call.
  Value range: "On", "Off".
  Default: "On".
- **Ring delay**: Time interval in seconds after which the line starts ringing on an incoming call.
  Default: 0.
- **Selection order**: Priority assigned to the line for the selection of an outgoing line.
  Default: 0.
- **Address**: Address/phone number which has a corresponding entry on the SIP server/ registrar.
- **Realm**: Domain wherein user id and password are valid.
- **User Identifier**: User name for authentication with the SIP server.
- **Password**: Password for authentication with the SIP server.

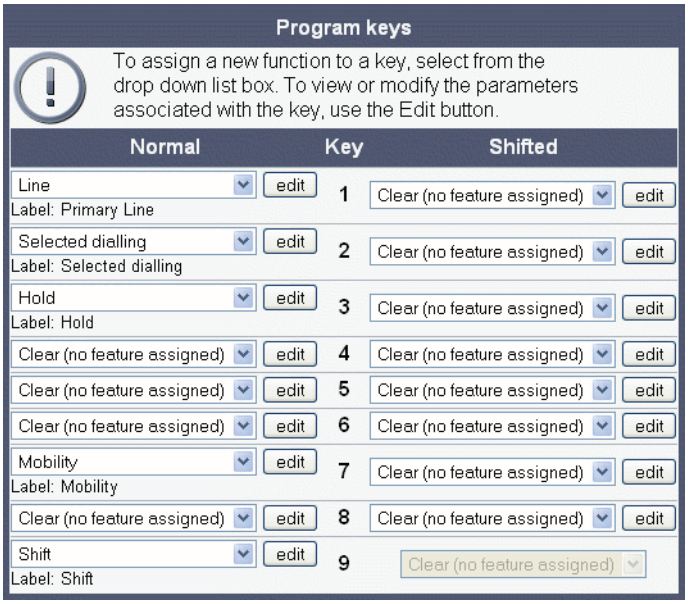
- **Shared type**: Determines whether the line is a shared line (shared by multiple endpoints) or a private line (only available for this endpoint).
  Value range: "shared", "private", "unknown".
  Default: "shared".
- **Allow in Overview**: Determines whether the line appears in the phone's line overview.
  Value range: "Yes", "No".
  Default: "Yes".

A new line key can only be added by use of the WBM or, preferably, the DLS. Once a line key exists, it can also be configured by the local menu.

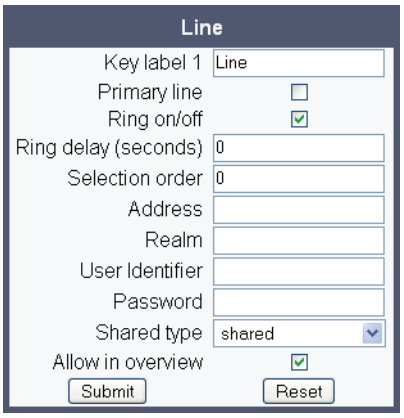
Administration via WBM

1. Invoke the "Phone keys" dialog and select "line" in the pulldown menu of the key you want to configure. Next, press "Edit...".

Features > Program keys



2. In the "Line" dialog, set the specific parameters for the line key.



Administration via Local Phone

The configuration of a line via Local phone is only possible when the line key has been created via Web interface or DLS before.

- Administration
  - System
    - Features
      - Configuration
        - Keyset Lines
          - Details For Keyset Line <xx>
            - **Address**
            - **Ring on/off**
            - **Selection order**

3.7.2 Configure Keyset Operation

The following parameters provide general settings which are common for all keyset lines.

The **Rollover ring** setting will be used in the case that, during an active call, an incoming call arrives on a different line. If "no ring" is selected, the incoming call will not initiate a ring. If "alert ring" is selected, a special alert ringtone is activated on an incoming call; "alert beep" selects a beep instead of a ringtone. "Standard ringtone" selects the default ringtone.

LED on registration determines whether the line LEDs will be lit for a few seconds if they have been registered successfully with the SIP server on phone startup.

The **Originating line preference** parameter determines which line will be used when the user goes off-hook or starts on-hook dialing.

When a terminating call exists, the terminating line preference takes priority over originating line preference.

The following preferences can be configured:

- "idle line": An idle line is selected. The selection is based on the **Hunt ranking** parameter assigned to each line (see Section 3.7.1, “Line key configuration”).
- "primary": The designated Primary Line is always selected for originating calls.
- "last": The line selected for originating calls is the line that has been used for the last call (originating or terminating).
- "none": The user manually selects a line by pressing its line key before going off-hook, or by pressing the speaker key, to originate a call. Manual line selection overrides automatic line preferences.

The **Terminating line preference** parameter decides which terminating line, i. e. line with an incoming call, is selected when the user goes off-hook.

The following preferences can be configured:

- "ringing line": The line in the alerting or audible ringing state is automatically selected when the user goes off-hook. In the case of multiple lines alerting or ringing, the lines are selected on the one that has been alerting the longest.
- "ringing PLP": The line in the alerting or audible ringing state is automatically selected when the user goes off-hook. However, if the prime line is alerting, it is given priority.
- "incoming": The earliest line to start audible ringing is selected, or else the earliest alerting (ringing suppression ignored) line is selected.
- "incoming PLP": The earliest line to start audible ringing is selected, or else the earliest alerting (ringing suppression ignored) line is selected. However, if the prime line is alerting, it is given priority.

- "none": To answer a call, the user manually selects a line by pressing its line key before going off-hook, or by pressing the speaker key. Manual line selection overrides automatic line preferences.

Line action mode determines the consequence for an established connection when the line key is pressed. If "hold" is selected, the call currently active is set to hold as soon as the line key is activated. The user has two options: 1) to reconnect to the remote phone by pressing the line key that corresponds to that call, or 2) to initiate another call from the newly selected line. If "release" is selected, the previously established call is ended.

If **Show Focus** is checked, the LED of a line key flutters when the line is in use. If it is not checked, the line key is lit steady when it is in use.

The **Reservation timer** sets the period after which the reservation of a line is canceled. A line is automatically reserved for the keyset whenever the user has selected a line for an outgoing call and hears a dial tone. The reservation of a line is accomplished by the HiPath 8000 server, which notifies all the endpoints sharing this line. If set to 0, the reservation timer is deactivated.

Forward indication activates or deactivates the indication of station forwarding, i. e. the forwarding function of the HiPath 8000. If **Forward indication** is activated and station forwarding is active for the corresponding line, the LED of the line key blinks.

Preselect mode determines the phone's behaviour when a call is active, and another call is ringing. If the parameter is set to "Single button", the user can accept the call a single press on the line key. If it is set to "Preselection", the user must first press the line key to select it and then press it a second time to accept the call. In both cases, the options for a ringing call are presented to the user: "Accept", "Reject", "Deflect".

Preselect timer sets the timeout for an incoming call. After the timeout has expired, the call is no longer available.

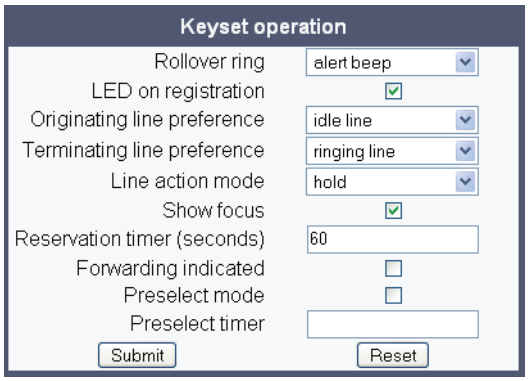
Data required

- **Rollover ring**: Determines if a ringtone will signal an incoming call while a call is active.
  Value range: "No ring", "Alert beep", "Alert ring".
  Default: "Alert beep".
- **LED on registration**: Determines if line LEDs will signal SIP registration.
  Value range: "Yes", "No".
  Default: "Yes".
- **Originating line preference**: Selects the line to be used for outgoing calls.
  Value range: "Idle line", "Primary", "Last", "None".
  Default: "Idle line".
- **Terminating line preference**: Determines which line with an incoming call shall be selected for answering.
  Value range: "Ringing line", "Incoming", "Incoming PLP", "Ringing PLP", "None".
  Default: "Idle line".

- **Line action mode**: Determines the consequence for an established connection when the line key is pressed.
  Value range: "Hold", "Release".
  Default: "Hold".
- **Show focus**: Determines whether the line Key LED blinks or is steady when it is in use.
  Value range: "Yes", "No".
  Default: "Yes".
- **Reservation timer**: Sets the period in seconds after which a line reservation is cancelled. If set to 0, the reservation timer is deactivated.
  Default: 60.
- **Forward indication**: Activates or deactivates the indication of station forwarding.
  Value range: "Yes", "No".
  Default: "No".
- **Preselect mode**: Determines whether an incoming call is accepted by a single press on the corresponding line key or a double press is needed.
  Value range: "Single button", "Preselection".
  Default: "Single button".
- **Preselect timer**: Sets the timeout in seconds for accepting an incoming call.

Administration via WBM

System > Features > Keyset Operation



Administration via Local Phone

- Administration
  - System
    - Features
      - Keyset operation
        - **Rollover ring**
        - **LED on registration**
        - **Originating line preference**
        - **Terminating line preference**
        - **Line action mode**
        - **Show focus**
        - **Reservation timer**
        - **Forward indicated**
        - **Preselect mode**
        - **Preselect timer**

3.7.3 Direct Station Select (DSS)

This feature is available only on OpenStage 40/60/80, and requires HiPath V 3.0.

A DSS key is a special variant of a line key. It enables a direct connection to a target phone, allowing the user to pick up or forward a call alerting the DSS target and make/complete a call to the DSS target.

3.7.3.1 General DSS Settings

These parameters define the behaviour of all DSS keys.

Generally, it is advisable to restrict the user's possibilities to modify line keys, including DSS keys. This can be achieved solely by the DLS. For further instructions, see the DLS Administration Guide.

If the user picks up an incoming call for the DSS target by pressing the associated DSS key, the call is forwarded to the user's primary line. Thereafter, the user's phone rings, and the user can accept the call.

To enable the immediate answering of a call via the DSS key, **Allow auto-answer** in the user menu must be activated. The complete path on the WBM is:
User Pages > Configuration > Incoming calls > CTI calls > Allow auto-answer.

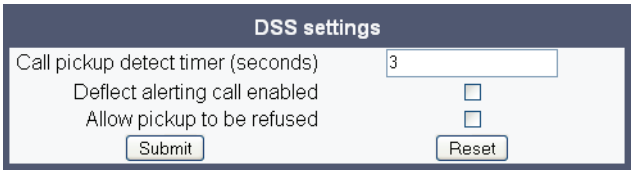
The value of **Call pickup detect timer (seconds)** determines the time interval, within which the call must be present at the primary line. If the interval is exceeded, forwarding will not be tried any longer. The default is 3.

If **Deflecting call enabled** is checked, the user can forward an alerting call to the DSS target by pressing the DSS key. The default is "No".

If **Allow pickup to be refused** is checked, the user is enabled to reject a call alerting on the line associated with the DSS key. The default is "No".

Administration via WBM

System > Features > DSS Settings



Administration via Local Phone

```
└--- Administration
     └--- System
          └--- Features
               └--- Feature Access
                    └--- Call establish
                         |--- Deflect to DSS
                         └--- Refuse DSS pickup
```

```
└--- Administration
     └--- System
          └--- Features
               └--- Configuration
                    └--- General
                         └--- DSS Pickup timer
```

3.7.3.2 Settings for a DSS key

The **Key label <n>** parameter provides the DSS key with a label that is displayed on the graphic display on a OpenStage 60/80 phone. The label is also user configurable.

Address contains the call number of the line associated with the DSS key.

The **Realm** parameter stores the SIP Realm of the line associated with the DSS key.

User Identifier gives the SIP user ID of the line associated with the DSS key.

Password provides the password corresponding to the SIP user ID.

The **Outgoing calls** parameter determines the behaviour of a call over the DSS line at the target phone. If set to "Direct", any forwarding and Do not Disturb settings on the target phone will be overridden, so that a call will always alert. If set to Line type is set to "Normal", this is not the case, and the call will be treated like a regular call.

Action on calls defines the handling of an active call when pressing the DSS key. If set to "Consult", the user has an option to start a consultation with the DSS target. If set to "Transfer", the user can only transfer the call to the DSS target. If "No action" is selected, pressing the DSS key will have no effect.

When **Allow in Overview** is set to "Yes", the line corresponding to the DSS key will be visible in the line overview on the phone's display.

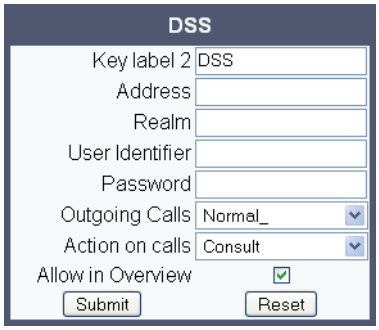
Data required

- **Key label <key number>**: Label to be displayed on the display.
  Default: "DSS".
- **Address**: SIP Address of Record of the destination that is assigned to the DSS key.
- **Realm**: SIP Realm of the DSS destination.

- **User ID**: SIP user ID of the DSS destination.
- **Password**: Password corresponding to the SIP user ID.
- **Outgoing calls**: Determines whether forwarding and DND at the target phone will be overridden on a DSS call.
  Value range: "Normal", "Direct".
  Default: "Normal".
- **Action on calls**: Handling of an active call when pressing the DSS key. "Consult": the user can start a consultation with the DSS target; "Transfer": the user can transfer the call to the DSS target.
  Value range: "Consult", "Transfer", "No action".
  Default: "Consult".
- **Allow in Overview**: Determines whether the line appears in the phone's line overview.
  Value range: "Yes", "No".
  Default: "Yes".

Administration via WBM

System > Features > Program keys > [edit]

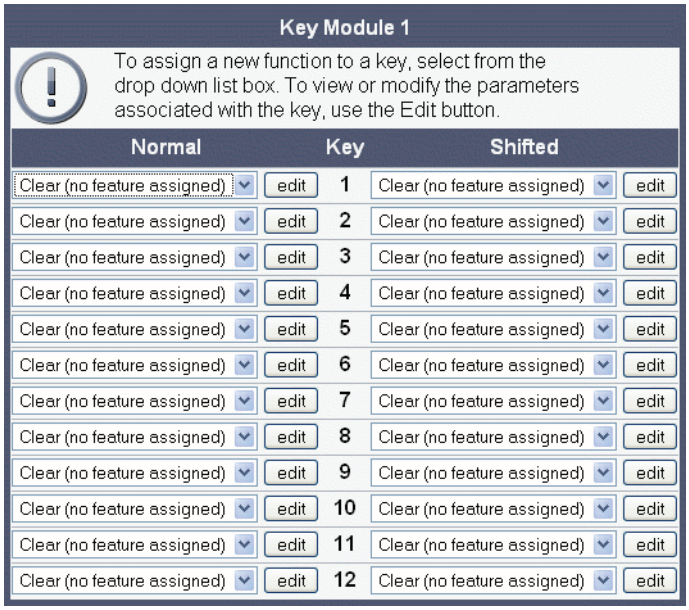


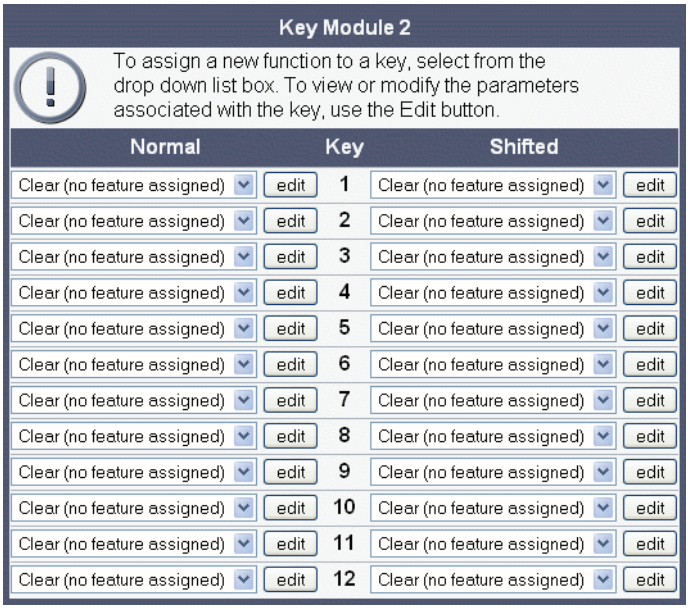
3.7.4 Key Modules

A Key module provides 12 additional program keys. It is available for the OpenStage 40, 60 and 80. A maximum of 2 key modules can be connected to one phone. The configuration of a key on the key module is just the same as the configuration of a phone key.

Administration via WBM

System > Features > Key module 1/2





3.8 Dialing

3.8.1 Canonical Dialing Configuration

Call numbers taken from a directory application, LDAP for instance, are mostly expressed in canonical format. Moreover, call numbers entered into the local phone book are automatically converted and stored in canonical format, thereby adding "+", **Local country code**, **Local national code**, and **Local enterprise number** as prefixes. If, for instance, the user enters the extension "1234", the local country code is "49", the local national code is "89", and the local enterprise number is "722", the resulting number in canonical format is "+49897221234".

For generating an appropiate dial string, a conversion from canonical format to a different format may be required. The following parameters determine the local settings of the phone, like **Local country code** or **Local national code**, and define rules for converting from canonical format to the format required by the PBX.

To enable the number conversion, all parameters not marked as optional must be provided, and the canonical dial lookup settings must be configured (see Section 3.8.2, “Canonical Dial Lookup”).

Data required

- **Local country code**: E.164 Country code, e.g. "49" for Germany, "44" for United Kingdom. Maximum length: 5.
- **National prefix digit**: Prefix for national connections, e.g. "0" in Germany and United Kingdom. Maximum length: 5.
- **Local national code**: Local area code or city code, e.g. "89" for Munich, "20" for London. Maximum length: 6.
- **Minimal local number length**: Minimum number of digits in a local PSTN number, e.g. 3335333 = 7 digits.
- **Local enterprise number**: Number of the company/PBX wherein the phone is residing. Maximum length: 10. (Optional)
- **PSTN access code**: Access code used for dialing out from a PBX to a PSTN. Maximum length: 10. (Optional)
- **International access code**: International prefix used to dial to another country, e.g. "00" in Germany and United Kingdom. Maximum length: 5.
- **Operator codes**: List of extension numbers for a connection to the operator. The numbers entered here are not converted to canonical format. Maximum length: 50. (Optional)
- **Emergency number**: List of emergency numbers to be used for the phone. If there are more than one numbers, they must be separated by commas. The numbers entered here are not converted to canonical format. Maximum length: 50. (Optional)

From V1R4.x on, these emergency numbers can also be dialed when the phone is locked, in line with the emergency number configured in **Features** > **Configuration** (see Section 3.5.2, “Emergency and Voice Mail”).

- **Initial extension digits** / **Initial digits**: List of initial digits of all possible extensions in the local enterprise network. When a call number could not be matched as a public network number, the phone checks if it is part of the local enterprise network. This is done by comparing the first digit of the call number to the value(s) given here. If it matches, the call number is recognized as a local enterprise number and processed accordingly.
If, for instance, the extensions 3000-5999 are configured in the HiPath 8000, each number will start with 3, 4, or 5. Therefore, the digits to be entered are 3, 4, 5.
- **Internal numbers**

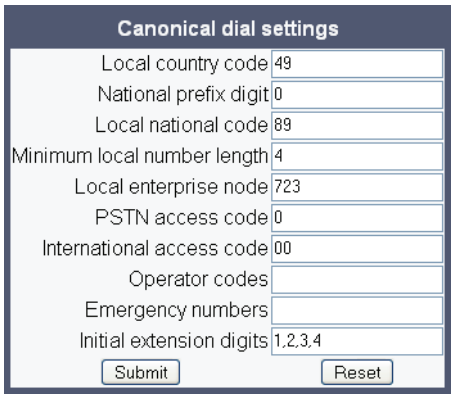
To enable the phone to discern internal numbers from external numbers, it is crucial that a canonical lookup table is provided (Section 3.8.2, “Canonical Dial Lookup”).

  - "Local enterprise form": Default value. Any extension number is dialled in its simplest form. For an extension on the local enterprise node, the node ID is omitted. If the extension is on a different enterprise node, then the appropriate node ID is prefixed to the extension number. Numbers that do not correspond to an enterprise node extension are treated as external numbers.
  - "Always add node": Numbers that correspond to an enterprise node extension are always prefixed with the node ID, even those on the local node. Numbers that do not correspond to an enterprise node extension are treated as external numbers.
  - "Use external numbers": All numbers are dialled using the external number form.
- **External numbers**
  - "Local public form": Default value. All external numbers are dialled in their simplest form. Thus a number in the local public network region does not have the region code prefix. Numbers in the same country but not in the local region are dialled as national numbers. Numbers for a different country are dialled using the international format.
  - "National public form": All numbers within the current country are dialled as national numbers, thus even local numbers will have a region code prefix (as dialling from a mobile). Numbers for a different country are dialled using the international format.
  - "International form": All numbers are dialled using their full international number format.
- **External access code**
  - "Not required": The access code to allow a public network number to be dialled is not required.

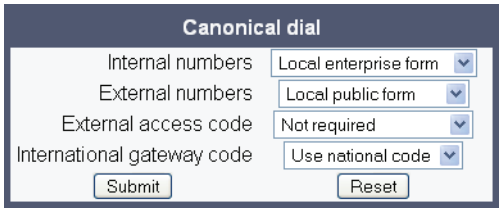
  - "For external numbers": Default value. All public network numbers will be prefixed with the access code that allows a number a call to be routed outside the enterprise network. However, international numbers that use the + prefix will not be given access code.
- **International gateway code**:
  - "Use national code": Default value. All international formatted numbers will be dialled explicitly by using the access code for the international gateway to replace the "+" prefix.
  - "Leave as +": All international formatted numbers will be prefixed with "+".

Administration via WBM

Local functions > Locality > Canonical dial settings



Local functions > Locality > Canonical dial



Administration via Local Phone

- Administration
  - Local Functions
    - Locality
      - Canonical dial settings
        - **Local country code**
        - **National prefix digit**
        - **Local national code**
        - **Minimum local number length**
        - **Local enterprise node**
        - **PSTN access code**
        - **International access code**
        - **Operator code**
        - **Emergency number**

- Administration
  - Local Functions
    - Locality
      - Canonical dial
        - **Internal numbers**
        - **External numbers**
        - **External access code**
        - **International gateway**

3.8.2 Canonical Dial Lookup

The parameters given here are important for establishing outgoing calls and for recognizing incoming calls.

In the local phonebook, and, mostly, in LDAP directories, numbers are stored in canonical format. In order to generate an appropriate dial string according to the settings in **Internal numbers** and **External numbers** (-> Section 3.8.1), internal numbers must be discerned from external numbers. The canonical lookup table provides patterns which allow for operation.

Furthermore, these patterns enable the phone to identify callers from different local or international telephone networks by looking up the caller's number in the phone book. As incoming numbers are not always in canonical format, their composition must be analyzed first. For this purpose, an incoming number is matched against one or more patterns consisting of country codes, national codes, and enterprise nodes. Then, the result of this operation is matched against the entries in the local phone book.

To make sure that canonical dial lookup works properly, at least the following parameters of the phone must be provided:

- **Local country code** (-> Section 3.8.1)
- **Local area code** (-> Section 3.8.1)
- **Local enterprise code** (-> Section 3.8.1)

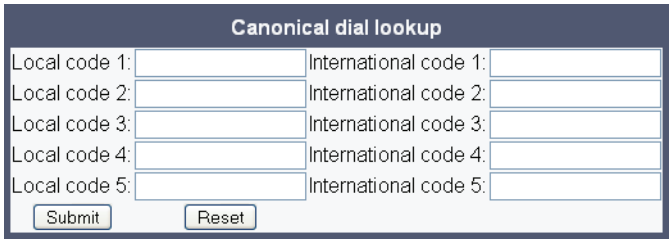
Up to 5 patterns can be defined. The **Local code 1 ... 5** parameters define up to 5 different local enterprise nodes, whilst **International code 1... 5** define up to 5 international codes, that is, fully E.164 call numbers for use in a PSTN.

Data required

- **Local code 1 ... 5**: Local enterprise code for the node/PBX the phone is connected to. Example: "722" for Siemens Munich.
- **International code 1 ... 5**: Sequence of "+", local country code, local area code, and local enterprise node corresponding to to one or more phone entries. Example: "+4989722" for Siemens Munich.

Administration via WBM

Locality > Canonical dial lookup



Administration via Local Phone

- Administration
  - Local Functions
    - Locality
      - Canonical Dial Lookup
        - **Local code 1**
        - **International code 1**
        - **Local code 2**
        - **International code 2**
        - **Local code 3**
        - **International code 3**
        - **Local code 4**
        - **International code 4**
        - **Local code 5**
        - **International code 5**

3.9 Mobility

The Mobility feature requires the HiPath Deployment Severice (DLS). If the phone is mobility enabled by the DLS, a mobile user can log on to the phone and thereby have his own user settings transferred to the phone. These user data are stored in the DLS database and include, for instance, SIP registration settings, dialing properties, key layouts, as well as the user's phonebook.

If the mobile user changes some settings, the changed data is sent to the DLS server. This ensures that his user profile is updated if necessary.

If **Unauthorized logoff trap** is set to "Yes", a message is sent to the SNMP server if an unauthorized attempt is made to log off the mobile user.

Logoff trap delay defines the time span in seconds between the unauthorized logoff attempt and the trap message to the SNMP server.

Timer med priority determines the time span in seconds between a change of user data in the phone and the transfer of the changes to the DLS server.

The **Mobility feature** parameter indicates whether the mobility feature is enabled by the DNS or not.

Data required

- **Unauthorized logoff trap**: An SNMP trap is sent on an unauthorized logoff attempt.
  Value range: "Yes", "No".
  Default: "No".
- **Logoff trap delay**: Time span in seconds between the unauthorized logoff attempt and the SNMP trap.
  Default: 300.
- **Timer med priority**: Time span in seconds between a data change in the phone and its transfer to the DLS server.
  Default: 60.
- **Mobility feature**: Indicates whether the mobility feature is enabled.

Administration via Local Phone

```
└── Administration
    └── Mobility
        ├── Unauthorized logoff trap
        ├── Logoff trap delay
        ├── Timer med priority
        └── Mobility feature
```

3.10 Transferring Phone Software, Application and Media Files

New software images, hold music, picture clips for phonebook entries, LDAP templates, company logos, screensaver images, and ringtones can be uploaded to the phone via DLS (Deployment Service) or WBM (Web Based Management).

For all user data, which includes files as well as phonebook content, the following amounts of storage place are available:

- OpenStage 20/40: 4 MB
- OpenStage 60/80: 8 MB

3.10.1 FTP/HTTPS Server

There are no specific requirements regarding the FTP server for transferring files to the OpenStage phone. Any FTP server providing standard functionality will do.

3.10.2 Common FTP/HTTPS Settings

For each one of the various file types, e.g. phone software, hold music, and picture clips, specific FTP/HTTPS access data can be defined. If some or all file types have the parameters **Download method**, **Server**, **Server port**, **Account**, **Username**, **FTP path**, and **HTTPS baser URL** in common, they can be specified here. These settings will be used for a specific file type if its **Use defaults** parameter is set to "Yes".

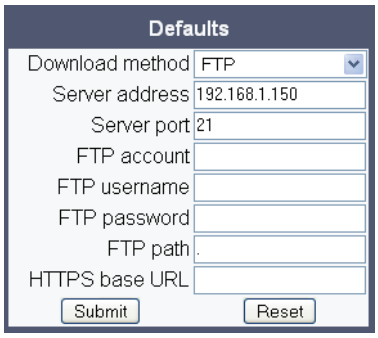
If **Use defaults** is activated for a specific file type, any specific settings for this file type are overridden by the defaults.

Data required

- **Download method**: Selects the protocol to be used.
  Value range: "FTP", "HTTPS".
  Default: "FTP".
- **Server address**: IP address or hostname of the FTP/HTTPS server in use.
- **Server port**: Port number of the FTP/HTTPS server in use.
  Default: 21.
- **FTP account**: Account at the server (if applicable).
- **FTP username**: User name for accessing the server.
- **FTP password**: Password corresponding to the user name.
- **FTP path**: Path of the directory containing the files.
- **HTTPS base URL**: IP address or hostname of the HTTPS server in use; only applicable if **Download method** is switched to "HTTPS".

Administration via WBM

File transfer > Defaults



Administration via Local Phone

- Administration
  - File Transfer
    - Defaults
      - **Download method**
      - **Server**
      - **Port**
      - **Account**
      - **Username**
      - **Password**
      - **FTP path**
      - **HTTPS base URL**

3.10.3 Phone Software

The firmware for the phone can be updated by downloading a new software file to the phone.

Do not disconnect the phone from the LAN or power unit during software update. An active update process is indicated by blinking LEDs and/or in the display.

3.10.3.1 FTP/HTTPS Access Data

If the default FTP/HTTPS Access settings (see Section 3.10.2, “Common FTP/HTTPS Settings”) are to be used, **Use default** must be set to "Yes", and only the **Filename** must be specified.

Data required (in every case)

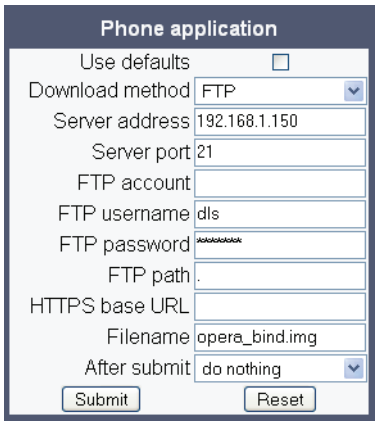
- **Use default**: Specifies whether the default FTP/HTTPS access settings shall be used. Value range: "Yes", "No".
  Default: "No".
- **Filename**: Specifies the file name of the phone software.

Data required (if not derived from Defaults)

- **Download method**: Selects the protocol to be used.
  Value range: "FTP", "HTTPS".
  Default: "FTP".
- **Server address**: IP address or hostname of the FTP/HTTPS server in use.
- **Server port**: Port number of the FTP/HTTPS server in use.
  Default: 21.
- **FTP account**: Account at the server (if applicable).
- **FTP username**: User name for accessing the server.
- **FTP password**: Password corresponding to the user name.
- **FTP path**: Path of the directory containing the files.
- **HTTPS base URL**: IP address or hostname of the HTTPS server in use; only applicable if **Download method** is switched to "HTTPS".

Administration via WBM

File transfer > Phone application



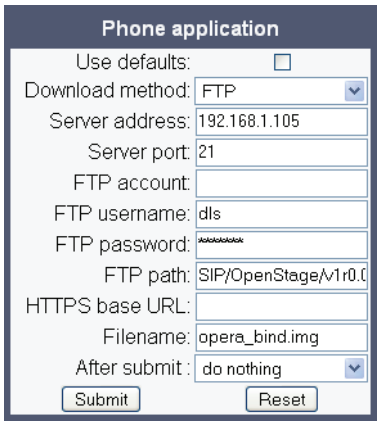
Administration via Local Phone

- Administration
  - File Transfer
    - Phone app
      - **Use default**
      - **Download method**
      - **Server**
      - **Port**
      - **Account**
      - **Username**
      - **Password**
      - **FTP path**
      - **HTTPS base URL**
      - **Filename**

3.10.3.2 Download/Update Phone Software

If applicable, phone software should be deployed using the Deployment Service (DLS). Alternatively, the download can be triggered from the web interface or from the Local phone menu. When the download has been successful, the phone will restart and boot up using the new software.

Start Download via WBM



In the **File transfer** > Phone application dialog, set **After submit** to "start download" and press the **Submit** button.

Start Download via Local Phone

1. In the administration menu, set the focus to **Phone app**.

└─ Administration
  └─ File Transfer
    └─ **Phone app**

2. Press the ➔ key. A context menu opens. In the context menu, select **Download**. The download will start immediately.

3.10.4 Music on Hold

If enabled by the user, the Music on Hold (MoH) sound file is played when a call is put on hold.

With V1R4.x upwards, the file size for a Music on Hold file is limited to 1MB. If the file is too large or the contents of the file are not valid, the file will not be stored in the phone.

The following formats for Music on Hold are supported:

- Proprietary Music on Hold format for optiPoint 410/420 phones
- WAV format. The recommended specifications are:
  - Audio format: PCM
  - Bitrate: 16 kB/sec
  - Sampling rate: 8 kHz
  - Quantization level: 16 bit.
- MIDI format.
- MP3 format (OpenStage 60/80 only). A bitrate of 48 kB/sec is recommended.

3.10.4.1 FTP/HTTPS Access Data

If the default FTP/HTTPS access settings (see Section 3.10.2, “Common FTP/HTTPS Settings”) are to be used, **Use Default** must be set to "Yes", and only the **Filename** must be specified.

Data required (in every case)

- **Use default**: Specifies whether the default FTP/HTTPS access settings shall be used. Value range: "Yes", "No".
  Default: "No".
- **Filename**: Specifies the file name of the phone software.

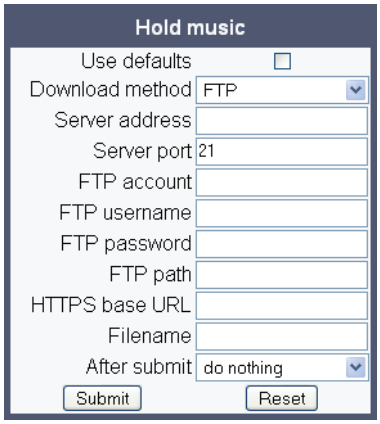
Data required (if not derived from Defaults)

- **Download method**: Selects the protocol to be used.
  Value range: "FTP", "HTTPS".
  Default: "FTP".
- **Server address**: IP address or hostname of the FTP/HTTPS server in use.
- **Server port**: Port number of the FTP/HTTPS server in use.
  Default: 21.
- **FTP account**: Account at the server (if applicable).
- **FTP username**: User name for accessing the server.

- **FTP password**: Password corresponding to the user name.
- **FTP path**: Path of the directory containing the files.
- **HTTPS base URL**: IP address or hostname of the HTTPS server in use; only applicable if **Download method** is switched to "HTTPS".

Administration via WBM

File transfer > Hold music



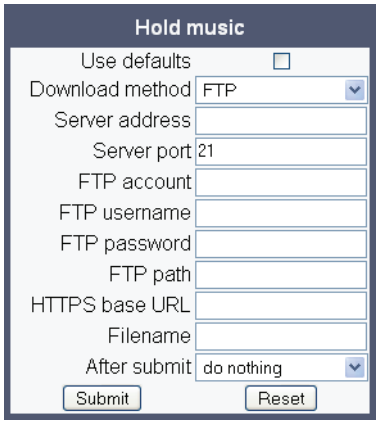
Administration via Local Phone

- Administration
  - File Transfer
    - Hold Music
      - **Use default**
      - **Download method**
      - **Server**
      - **Port**
      - **Account**
      - **Username**
      - **Password**
      - **FTP path**
      - **HTTPS base URL**
      - **Filename**

3.10.4.2 Download Music on Hold

If applicable, Music on Hold should be deployed using the Deployment Service (DLS). Alternatively, the download can be triggered from the web interface or from the local phone menu.

Start Download via WBM



In the **File transfer** > Hold music dialog, set **After submit** to "start download" and press the **Submit** button.

Start Download via Local Phone

1. In the administration menu, set the focus to **Hold Music**.

└── Administration
  └── File Transfer
    └── **Hold Music**

2. Press the ➔ key. A context menu opens. In the context menu, select **Download**. The download will start immediately.

3.10.5 Picture Clips

Picture clips are available only on OpenStage 60/80 phones.

With V1R4.x upwards, the file size for a picture clip is limited to 300 KB. If the file is too large or the contents of the file are not valid, the file will not be stored in the phone.

Picture Clips are small images used for displaying a picture of a person that is calling on a line. The supported file formats for picture clips are JPEG and PNG (recommended).

3.10.5.1 FTP/HTTPS Access Data

If the default FTP/HTTPS access settings (see Section 3.10.2, “Common FTP/HTTPS Settings”) are to be used, **Use default** must be set to "Yes", and only the **Filename** must be specified.

Data required (in every case)

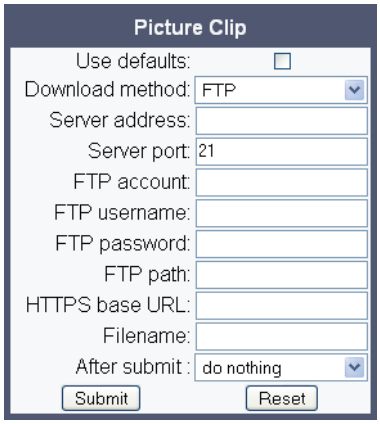
- **Use default**: Specifies whether the default FTP/HTTPS access settings shall be used. Value range: "Yes", "No".
  Default: "No".
- **Filename**: Specifies the file name of the phone software.

Data required (if not derived from Defaults)

- **Download method**: Selects the protocol to be used.
  Value range: "FTP", "HTTPS".
  Default: "FTP".
- **Server address**: IP address or hostname of the FTP/HTTPS server in use.
- **Server port**: Port number of the FTP/HTTPS server in use.
  Default: 21.
- **FTP account**: Account at the server (if applicable).
- **FTP username**: User name for accessing the server.
- **FTP password**: Password corresponding to the user name.
- **FTP path**: Path of the directory containing the files.
- **HTTPS base URL**: IP address or hostname of the HTTPS server in use; only applicable if **Download method** is switched to "HTTPS".

Administration via WBM

File transfer > Picture clip



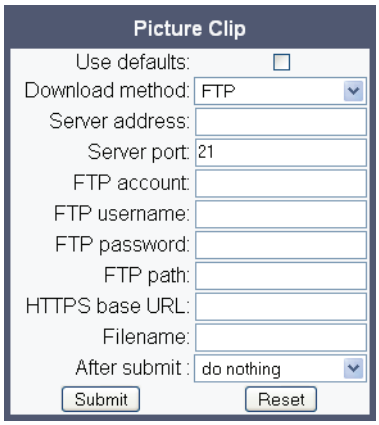
Administration via Local Phone

- Administration
  - File Transfer
    - Picture Clip
      - **Use default**
      - **Download method**
      - **Server**
      - **Port**
      - **Account**
      - **Username**
      - **Password**
      - **FTP path**
      - **HTTPS base URL**
      - **Filename**

3.10.5.2 Download Picture Clip

If applicable, picture clips should be deployed using the Deployment Service (DLS). Alternatively, the download can be triggered from the web interface or from the local phone menu.

Start Download via WBM



In the **File transfer** > Picture clip dialog, set **After submit** to "start download" and press the **Submit** button.

Start Download via Local Phone

1. In the administration menu, set the focus to **Picture clip**.

└--- Administration
  └--- File Transfer
    └--- **Picture clip**

2. Press the ➔ key. A context menu opens. In the context menu, select **Download**. The download will start immediately.

3.10.6 LDAP Template

LDAP is available only on OpenStage 60/80 phones.

The LDAP template is an ASCII text file that uses an allocation list to assign directory server attributes to input and output fields on an LDAP client. The LDAP template must be modified correctly for successful communication between the directory server and the LDAP client.

The OpenStage phone supports LDAPv3.

3.10.6.1 FTP/HTTPS Access Data

If the default FTP/HTTPS access settings (see Section 3.10.2, “Common FTP/HTTPS Settings”) are to be used, **Use default** must be set to "Yes", and only the **Filename** must be specified.

Data required (in every case)

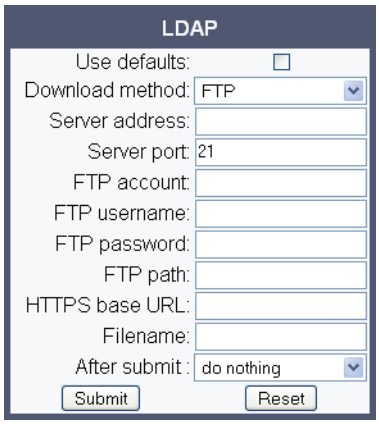
- **Use default**: Specifies whether the default FTP/HTTPS access settings shall be used. Value range: "Yes", "No".
  Default: "No".
- **Filename**: Specifies the file name of the phone software.

Data required (if not derived from Defaults)

- **Download method**: Selects the protocol to be used.
  Value range: "FTP", "HTTPS".
  Default: "FTP".
- **Server address**: IP address or hostname of the FTP/HTTPS server in use.
- **Server port**: Port number of the FTP/HTTPS server in use.
  Default: 21.
- **FTP account**: Account at the server (if applicable).
- **FTP username**: User name for accessing the server.
- **FTP password**: Password corresponding to the user name.
- **FTP path**: Path of the directory containing the files.
- **HTTPS base URL**: IP address or hostname of the HTTPS server in use; only applicable if **Download method** is switched to "HTTPS".

Administration via WBM

File transfer > LDAP



Administration via Local Phone

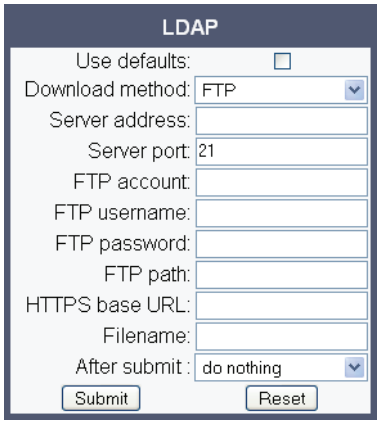
- Administration
  - File Transfer
    - LDAP
      - **Use default**
      - **Download method**
      - **Server**
      - **Port**
      - **Account**
      - **Username**
      - **Password**
      - **FTP path**
      - **HTTPS base URL**
      - **Filename**

3.10.6.2 Download LDAP Template

If applicable, LDAP templates should be deployed using the Deployment Service (DLS). Alternatively, the download can be triggered from the web interface or from the local phone menu.

The OpenStage phone supports LDAPv3.

Start Download via WBM



In the **File transfer** > LDAP dialog, set **After submit** to "start download" and press the **Submit** button.

Start Download via Local Phone

1. In the administration menu, set the focus to **LDAP**.

```
└── Administration
    └── File Transfer
        └── LDAP
```

2. Press the ➔ key. A context menu opens. In the context menu, select **Download**. The download will start immediately.

3.10.7 Logo

On OpenStage 40/60/80, a custom background image for the telephony interface can be supplied. In most cases, this will be the company logo.

On OpenStage 40, monochrome bitmap files (BMP) are supported. The ideal size is as follows:

- Width: 144 px
- Height: 32 px

On OpenStage 60/80, the supported file formats are JPEG and PNG. The ideal size values are is as follows:

OpenStage 60:

- Width: 240 px
- Height: 70 px

OpenStage 80:

- Width: 480 px
- Height: 148 px

If the size should deviate from these values, the image will appear skewed.

For guidance on creating a logo file for OpenStage 40/60/80, see Section 4.2, “How to Create Logo Files for OpenStage Phones”.

3.10.7.1 FTP/HTTPS Access Data

If the default FTP/HTTPS access settings (see Section 3.10.2, “Common FTP/HTTPS Settings”) are to be used, **Use default** must be set to "Yes", and only the **Filename** must be specified.

Data required (in every case)

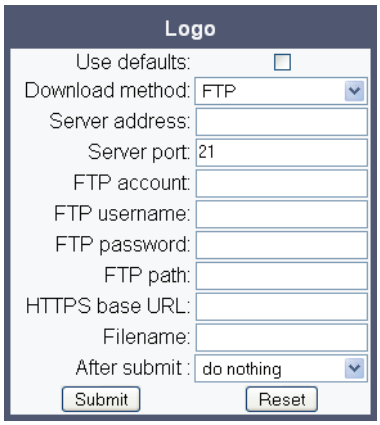
- **Use default**: Specifies whether the default FTP/HTTPS access settings shall be used. Value range: "Yes", "No".
  Default: "No".
- **Filename**: Specifies the file name of the phone software.

Data required (if not derived from Defaults)

- **Download method**: Selects the protocol to be used.
  Value range: "FTP", "HTTPS".
  Default: "FTP".
- **Server address**: IP address or hostname of the FTP/HTTPS server in use.
- **Server port**: Port number of the FTP/HTTPS server in use.
  Default: 21.
- **FTP account**: Account at the server (if applicable).
- **FTP username**: User name for accessing the server.
- **FTP password**: Password corresponding to the user name.
- **FTP path**: Path of the directory containing the files.
- **HTTPS base URL**: IP address or hostname of the HTTPS server in use; only applicable if **Download method** is switched to "HTTPS".

Administration via WBM

File transfer > Logo



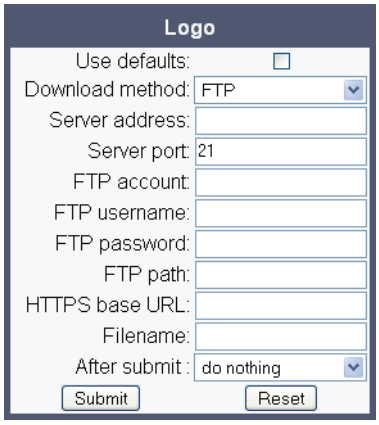
Administration via Local Phone

```
└--- Administration
     └--- File Transfer
          └--- Logo
               |--- Use default
               |--- Download method
               |--- Server
               |--- Port
               |--- Account
               |--- Username
               |--- Password
               |--- FTP path
               |--- HTTPS base URL
               └--- Filename
```

3.10.7.2 Download Logo

If applicable, logos should be deployed using the Deployment Service (DLS). Alternatively, the download can be triggered from the web interface or from the local phone menu.

Start Download via WBM



In the **File transfer** > Logo dialog, set **After submit** to "start download" and press the **Submit** button.

Start Download via Local Phone

1. In the administration menu, set the focus to **Logo**.

└--- Administration
  └--- File Transfer
    └--- **Logo**

2. Press the ➔ key. A context menu opens. In the context menu, select **Download**. The download will start immediately.

3.10.8 Screensaver

The screensaver is displayed when the phone is in idle mode. It performs a slide show consisting of images which can be uploaded using the web interface.

Screensavers are available only on OpenStage 60/80 phones.

With V1R4.x upwards, the file size for a screensaver image is limited to 300 KB. If the file is too large or the contents of the file are not valid, the file will not be stored in the phone.

For screensaver images, the following specifications are valid:

- Data format: JPG or PNG. JPG is recommended.
- Screen format: 4:3. The images are resized to fit in the screen, so that images with a width/height ratio differing from 4:3 will appear with deviant proportions.
- Resolution: The phone's screen resolution is the best choice for image resolution:
  - OpenStage 60: 320x240
  - OpenStage 80: 640x480

3.10.8.1 FTP/HTTPS Access Data

If the default FTP/HTTPS access settings (see Section 3.10.2, "Common FTP/HTTPS Settings") are to be used, **Use default** must be set to "Yes", and only the **Filename** must be specified.

Data required (in every case)

- **Use default**: Specifies whether the default FTP/HTTPS access settings shall be used. Value range: "Yes", "No".
  Default: "No".
- **Filename**: Specifies the file name of the phone software.

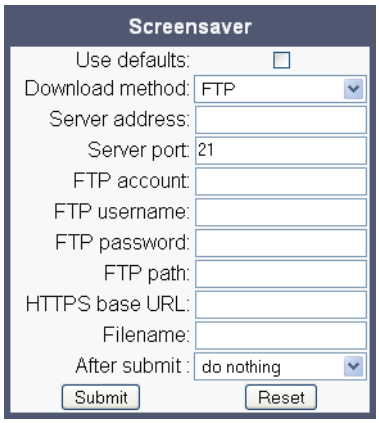
Data required (if not derived from Defaults)

- **Download method**: Selects the protocol to be used.
  Value range: "FTP", "HTTPS".
  Default: "FTP".
- **Server address**: IP address or hostname of the FTP/HTTPS server in use.
- **Server port**: Port number of the FTP/HTTPS server in use.
  Default: 21.
- **FTP account**: Account at the server (if applicable).

- **FTP username**: User name for accessing the server.
- **FTP password**: Password corresponding to the user name.
- **FTP path**: Path of the directory containing the files.
- **HTTPS base URL**: IP address or hostname of the HTTPS server in use; only applicable if **Download method** is switched to "HTTPS".

Administration via WBM

File transfer > Screensaver



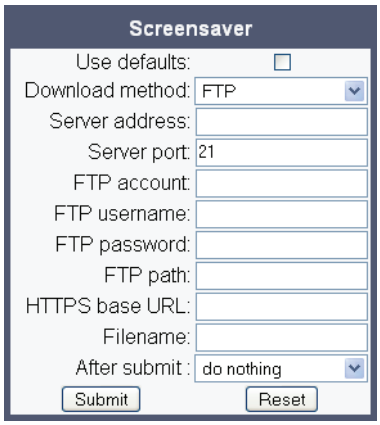
Administration via Local Phone

```
└--- Administration
     └--- File Transfer
          └--- Screensaver
               |--- Use default
               |--- Download method
               |--- Server
               |--- Port
               |--- Account
               |--- Username
               |--- Password
               |--- FTP path
               |--- HTTPS base URL
               └--- Filename
```

3.10.8.2 Download Screensaver

If applicable, screensavers should be deployed using the Deployment Service (DLS). Alternatively, the download can be triggered from the web interface or from the local phone menu.

Start Download via WBM



In the **File transfer** > Screensaver dialog, set **After submit** to "start download" and press the **Submit** button.

Start Download via Local Phone

1. In the administration menu, set the focus to **Screensaver**.

```
└── Administration
    └── File Transfer
        └── Screensaver
```

2. Press the ➔ key. A context menu opens. In the context menu, select **Download**. The download will start immediately.

3.10.9 Ringer File

Custom Ringtones can be uploaded to the phone.

With V1R4.x upwards, the file size for a ringer file is limited to 1 MB. IIf the file is too large or the contents of the file are not valid, the file will not be stored in the phone.

The following file formats are supported:

- WAV format. The recommended specifications are:
  - Audio format: PCM
  - Bitrate: 16 kB/sec
  - Sampling rate: 8 kHz
  - Quantization level: 16 bit
- MIDI format.
- MP3 format (OpenStage 60/80 only). The OpenStage 60/80 phones are able to play MP3 files from 32 kbit/s up to 320 kbit/s. As the memory for user data is limited to 8 MB, a constant bitrate of 48 kbit/sec to 112 kbit/s and a length of max. 1 minute is recommended. Although the phone software can play stereo files, mono files are recommended, as the phone has only 1 loudspeaker.
  See the following table for estimated file size (mono files):

Length	64 kbit/s	80 kbit/s	96 kbit/s	112 kbit/s
0:15 min	0,12 MB	0,15 MB	0,18 MB	0,21 MB
0:30 min	0,23 MB	0,29 MB	0,35 MB	0,41 MB
0:45 min	0,35 MB	0,44 MB	0,53 MB	0,62 MB
1:00 min	0,47 MB	0,59 MB	0,70 MB	0,82 MB

Tabelle 3-2

3.10.9.1 FTP/HTTPS Access Data

If the default FTP/HTTPS access settings (see Section 3.10.2, “Common FTP/HTTPS Settings”) are to be used, **Use default** must be set to "Yes", and only the **Filename** must be specified.

Data required (in every case)

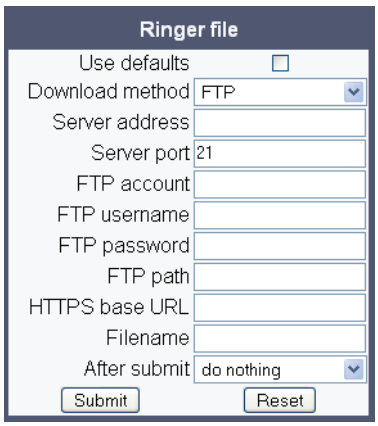
- **Use default**: Specifies whether the default FTP/HTTPS access settings shall be used. Value range: "Yes", "No".
  Default: "No".
- **Filename**: Specifies the file name of the phone software.

Data required (if not derived from Defaults)

- **Download method**: Selects the protocol to be used.
  Value range: "FTP", "HTTPS".
  Default: "FTP".
- **Server address**: IP address or hostname of the FTP/HTTPS server in use.
- **Server port**: Port number of the FTP/HTTPS server in use.
  Default: 21.
- **FTP account**: Account at the server (if applicable).
- **FTP username**: User name for accessing the server.
- **FTP password**: Password corresponding to the user name.
- **FTP path**: Path of the directory containing the files.
- **HTTPS base URL**: IP address or hostname of the HTTPS server in use; only applicable if **Download method** is switched to "HTTPS".

Administration via WBM

File transfer > Ringer file



Administration via Local Phone

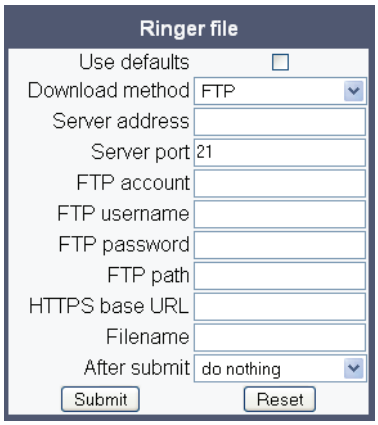
```
└── Administration
    └── File Transfer
        └── Ringer
            ├── Use default
            └── Download method
```

- **Server**
- **Port**
- **Account**
- **Username**
- **Password**
- **FTP path**
- **HTTPS base URL**
- **Filename**

3.10.9.2 Download Ringer File

If applicable, ringtone files should be deployed using the Deployment Service (DLS). Alternatively, the download can be triggered from the web interface or from the local phone menu.

Start Download via WBM



In the File transfer > Ringer dialog, set **After submit** to "start download" and press the **Submit** button.

Start Download via Local Phone

1. In the administration menu, set the focus to **Ringer**.

```
└── Administration
    └── File Transfer
        └── Ringer
```

2. Press the ➔ key. A context menu opens. In the context menu, select **Download**. The download will start immediately.

3.11 Corporate Phonebook: Directory Settings

3.11.1 LDAP

LDAP is available only on OpenStage 60/80 phones.

The Lightweight Directory Access Protocol enables access to a directory server via an LDAP client. Various personal information is stored there, e.g. the name, organisation and contact data of persons working in an organisation. When the LDAP client has found a person's data, e. g. by looking up the surname, the user can call this person directly using the displayed number.

The OpenStage phone supports LDAPv3.

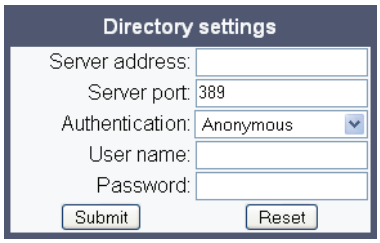
For connecting the phone's LDAP client to a LDAP server, the required access data must be configured. The parameters **Server address** and **Server port** specify the IP address and hostname as well as the port used by the LDAP server. If the **Authentication** is not set to "Anonymous", the user must authenticate himself with the server by providing an **User name** and a corresponding **Password**.

Data required

- **Server address**: IP address or hostname of the LDAP server.
- **Server port**: Port on which the LDAP server is listening for requests.
  Default: 389.
- **Authentication**: Authentication method used for connecting to the LDAP server. value range: "Anonymous", "Simple".
  Default: "Anonymous".
- **User name**: User name used for authentication with the LDAP server.
- **Password**: Password used for authentication with the LDAP server.

Administration via WBM

Local Functions > Directory settings



Administration via Local Phone

└--- Administration
  └--- Local Functions
    └--- Directory Settings
      |--- **LDAP server address**
      |--- **LDAP server port**
      |--- **LDAP authentication**
      |--- **LDAP user name**
      └--- **LDAP password**

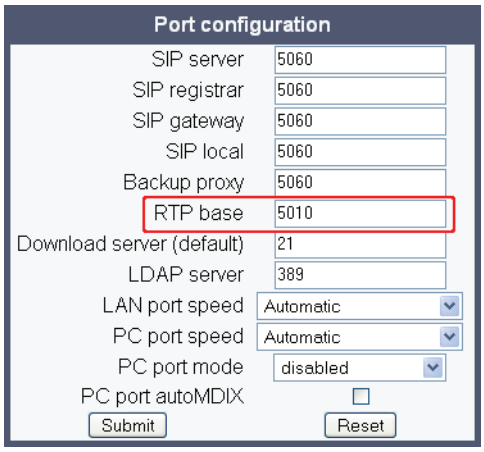
3.12 Speech

3.12.1 RTP Base Port

This parameter sets the port to be used for speech data, which is transmitted by RTP (Real-Time Transport Protocol). The default port number is 5010.

Administration via WBM

Network > Port Configuration



Administration via Local Phone

└--- Administration
  └--- Network
    └--- Port Configuration
      └--- **RTP base**

3.12.2 Codec Preferences

If **Silence suppression** is activated, the transmission of data packets is suppressed on no conversation, that is, if the user doesn't speak.

The OpenStage phone provides the codecs **G.711**, **G.722**, and **G.729**. When a SIP connection is established between two endpoints, the phones negotiate the codec to be used. The result of the negotiation is based on the general availability and ranking assigned to each codec. The administrator can allow or disallow a codec as well as assign a ranking number to it.

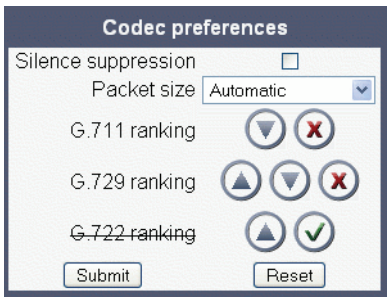
The **Packet size**, i. e. length in milliseconds, of the RTP packets for speech data, can be set to 10ms or 20ms or to automatic detection.

Data required

- **Silence suppression**: Suppression of data transmission on no conversation.
  Value range: "On", "Off".
  Default: "Off".
- **Packet size**: Size of RTP packets in milliseconds.
  Value range: "10 ms", "20ms", "Automatic".
  Default: "Automatic".
- **G.711**: Parameters for the G. 711 codec.
  Value Range: "Choice 1", "Choice 2", "Choice 3", "Disabled", "Enabled".
  Default: "Choice 1".
- **G.729**: Parameters for the G. 729 codec.
  Value Range: "Choice 1", "Choice 2", "Choice 3", "Disabled", "Enabled".
  Default: "Choice 2".
- **G.722**: Parameters for the G. 722 codec.
  Value Range: "Choice 1", "Choice 2", "Choice 3", "Disabled", "Enabled".
  Default: "Disabled".

Administration via WBM

Speech > Codec preferences



Administration via Local Phone

- Administration
  - Speech
    - Codec Preferences
      - **Silence suppression**
      - **Packet size**
      - **G.711**
      - **G.729**
      - **G.722**

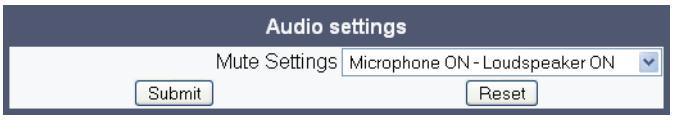
3.12.3 Audio Settings

The usage of microphone and speaker for speakerphone mode can be controlled by the administrator.

Both microphone and loudspeaker can be switched on or off separately. By default, both microphone and loudspeaker are switched on.

Administration via WBM

Speech > Audio Settings



Administration via Local Phone

```
└── Administration
    └── Speech
        └── Audio Settings
            ├── Disable microphone
            └── Disable loudspeech
```

3.13 Applications

3.13.1 XML Applications (OpenStage 60/80 with V1R3.x upwards)

3.13.1.1 Basic Setup/Configuration

The XML interface enables server-based applications with a set of GUI elements. The technologies commonly used in web applications can be used: Java Servlets, JSP, PHP, CGI etc., delivered by servers such as Tomcat, Apache, Microsoft IIS.

Xpressions is a special Unified Communications application which also uses the XML interface.

To set up a new XML application, enter the access data for the application on the server:

The **Display name** can be defined freely. This name will appear in the applications tab once the application is configured, and it will appear in a newy created tab when the application is running. With Xpressions, this value is predefined as "Xpressions".

The **Application name** is used by the phone software to identify the XML application running on the phone. With Xpressions, this value is predefined as "Xpressions".

The **Protocol** for exchanging XML data with the server-side program can be set to "HTTP" or "HTTPS".

The **Server address** is the IP address or domain name of the server which hosts the remote program. **Server port number** specifies the corresponding port.

Program name specifies the relative path to the servlet or to the first XML page of the application on the server. The relative path refers to the root directory for documents on the web server. The program name cannot be longer than 100 characters.

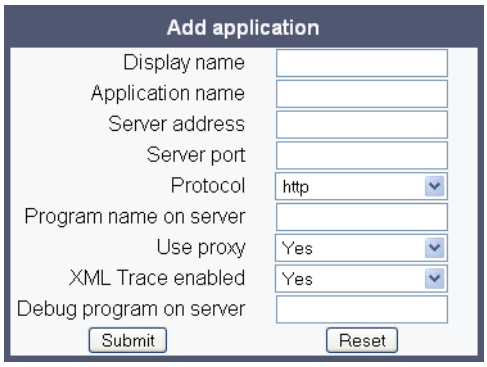
XML trace enabled determines whether debugging information is sent to a special debugging program on the remote server. The relative path for the debugging program is given by the **Debug program name** parameter.

Data required

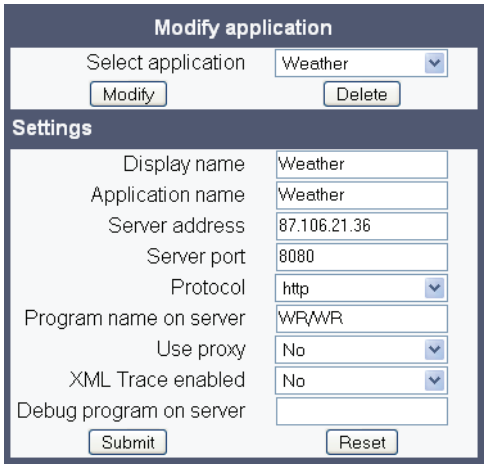
- **Display name**: Program name to be displayed on the phone.
  Value specifications:
  - It must be unique on the phone.
  - It cannot contain the '^' character.
  - It cannot not be empty.
  - Its length cannot not exceed 20 characters.
- **Application name**: Used internally to identify the XML application running on the phone.
  Value specifications:
  - It must be unique on the phone.
  - It cannot contain non-alphanumeric characters, spaces for instance.
  - The first character must be a letter.
  - It must not be empty.
  - Its length must not exceed 20 characters.
- **Protocol**: Communication protocol for the data exchange with the server.
  Value range: "HTTP", "HTTPS".
  Default: "HTTPS".
- **Server address**: IP address or domain/host name of the server that provides the application or the XML document.
- **Server port number**: Number of the port that the server uses to provide the application or XML document.
- **Program name**: Relative path to the servlet or to the first XML page of the application on the server.
- **XML trace enabled**: Enables or Disables the debugging of the XML application.
  Value range: "Yes", "No".
  Default: "No".
- **Debug program name**: The relative path to a special servlet that receives the debug information.

Administration via WBM

Applications > XML Applications > Add application



Applications > XML Applications > Modify application



Administration via Local Phone

```
└--- Administration
     └--- Applications
          └--- XML
               └--- Add application
                    |--- Display name
                    |--- Application name
                    |--- Server address
                    |--- Server port
                    |--- Protocol
                    |--- Program name
                    |--- XML trace enabled
                    └--- Debug program name
```

3.13.1.2 HTTP Proxy

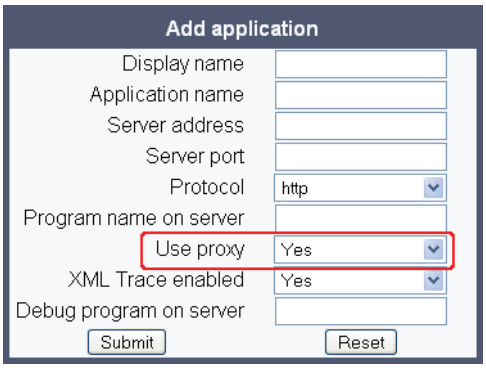
The HTTP data transfer between the phone and the server on which the remote program is running can be handled be an HTTP proxy, if desired.

First, the proxy itself must be configured. Enter the IP address of the proxy it in the Network > IP configuration > HTTP proxy parameter, and the corresponding port in the Network > Port configuration > HTTP proxy parameter.

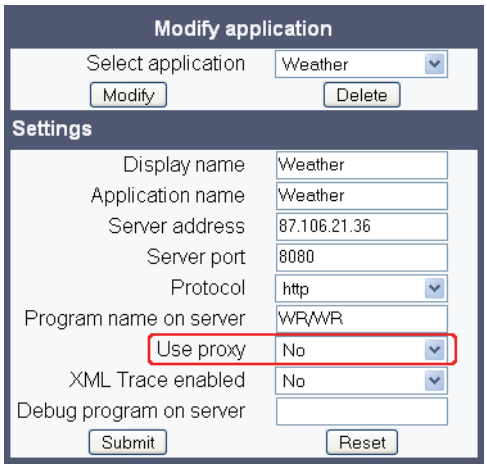
Use proxy enables or disables the use of the proxy. If disabled, the phones connects directly to the server. By default, the use of a proxy is disabled.

Administration via WBM

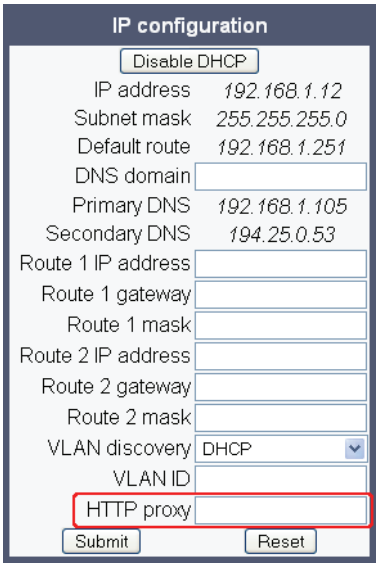
Applications > XML Applications > Add application



Applications > XML Applications > Modify application



Network > IP Configuration



Administration via Local Phone

```
└── Administration
    └── Applications
        └── XML
            ├── Add application
            │   └── Use proxy
            └── Add Xpressions
                └── Use proxy
```

```
└── Administration
    └── Network
        └── IP Configuration
            └── HTTP proxy
```

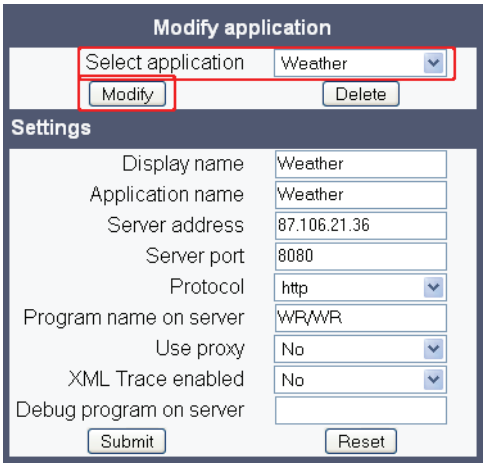
```
└── Administration
    └── Network
        └── Port configuration
            └── HTTP proxy
```

3.13.1.3 Modify an Existing Application

An existing application can be modified by changing its parameters. Please ensure to select the desired application before changing the parameters.

Administration via WBM

Applications > XML applications > Modify application



Administration via Local Phone

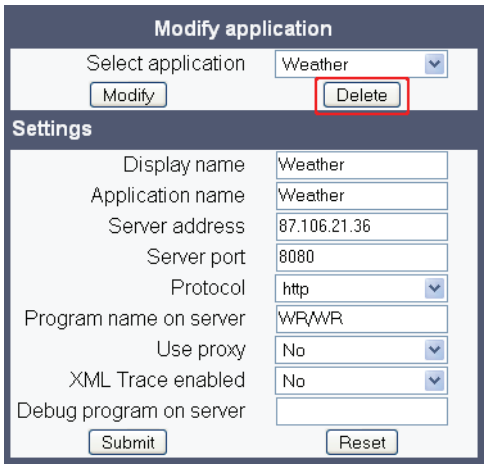
```
└--- Administration
     └--- Applications
          └--- XML
               └--- <Application to be modified>
                    |--- Display name
                    |--- Application name
                    |--- Server address
                    |--- Server port
                    |--- Protocol
                    |--- Program name
                    |--- XML trace enabled
                    └--- Debug program name
```

3.13.1.4 Remove an Existing Application

An existing application can be removed. Please ensure to select the desired application before changing the parameters.

Administration via WBM

Applications > XML applications > Modify application



Administration via Local Phone

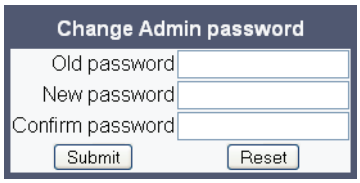
- Administration
  - Applications
    - XML
      - <Application to be modified>
        - **Display name**
        - **Application name**
        - **Server address**
        - **Server port**
        - **Protocol**
        - **Program name**
        - **XML trace enabled**
        - **Debug program name**

3.14 Password

The passwords for user and administrator can be set here. They have to be confirmed after entering. The factory setting is "123456"; it should be changed after the first login.

Administration via WBM

Authentication > Change Admin password



Authentication > Change User password

Administration via Local Phone

```
└--- Administration
     └--- Password
          |--- Admin
          |--- Confirmation
          |--- User
          └--- Confirmation
```

3.15 Troubleshooting: Lost Password

If the administration and/or user password is lost, and there is no DLS available, new passwords must be provided. For this purpose, a factory reset is necessary. Take the following steps to initiate a factory reset:

1. On the phone, press the ☰ key to activate the administration menu (the ☰ key toggles between the user's configuration menu and the administration menu).
2. Press the number keys 2-8-9 simultaneously. The factory reset menu opens.
3. In the input field, enter the special password for factory reset: "124816".
4. Confirm by pressing OK.

3.16 Factory Reset

This function resets all parameters to their factory settings. A special reset password is required for this operation: "124816".

Administration via WBM

Maintenance > Factory reset

Administration via Local Phone

└--- Administration
  └--- Maintenance
    └--- **Factory reset**

3.17 Diagnostics

3.17.1 Display General Phone Information

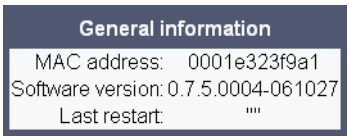
General information about the status of the phone can be displayed if desired.

Displayed Data

- **MAC address**: Shows the phone's MAC address.
- **Software version**: Displays the version of the phone's firmware.
- **Last restart**: Shows date and time of the last reboot.

Display on the WBM

General information



Display on the Local Phone

└--- Administration
  └--- General Information
    |--- **MAC address**
    |--- **Software version**
    └--- **Last restart**

3.17.2 LAN Monitoring

The LAN port mirror facility allows for monitoring all network traffic at the phone's LAN port. For further information, see Section 3.2.1, "LAN Port Settings".

Additionally, there is a possibility to monitor LAN traffic and port settings in the Local user menu:

- User
  - Network information
    - **IP address**
    - **WBM URL**
    - **DNS domain**
    - **LAN RX**
    - **LAN TX**
    - **PC RX**
    - **PC TX**
    - **LAN autonegotiated**
    - **LAN information**
    - **PC autonegotiated**
    - **PC information**

3.17.3 IP Tests

For network diagnostics, the OpenStage phone can ping any host or network device to determine whether it is reachable. Additionally, the IP route to a host or network device can be traced using the traceroute tool contained in the phone software.

The **Pre Defined Ping tests** provide pinging for a pre-defined selection of servers: DLS, SIP server, and SIP registrar.

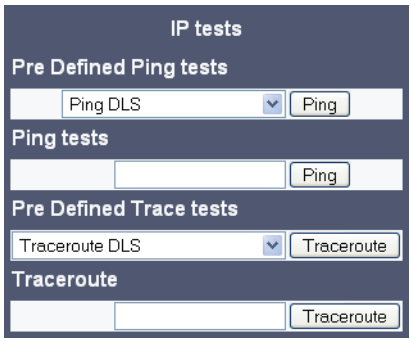
Ping tests enables the pinging of a random IP address.

The **Pre Defined Trace tests** provide traceroute tests for a pre-defined selection of servers: DLS, SIP server, and SIP registrar.

Traceroute enables traceroute tests for a random IP address.

Administration via WBM

Diagnostics > Miscellaneous > IP tests

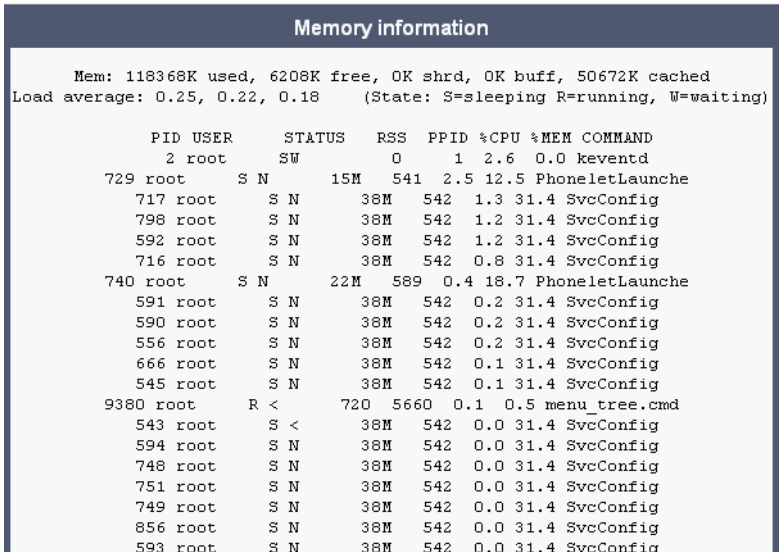


3.17.4 Process and Memory Information

The processes currently running on the phone's operating system as well as their CPU and memory usage can be monitored here. 100 processes are displayed on the web page. For further information, please refer to the documentation of the "top" command for Unix/Linux systems.

Administration via WBM

Diagnostics > **Miscellaneous** > Memory information


Memory information
Mem: 118368K used, 6208K free, 0K shrd, 0K buff, 50672K cached
Load average: 0.25, 0.22, 0.18 (State: S=sleeping R=running, W=waiting)
PID USER STATUS RSS PPID %CPU %MEM COMMAND
2 root SW 0 1 2.6 0.0 keventd
729 root S N 15M 541 2.5 12.5 PhoneletLaunche
717 root S N 38M 542 1.3 31.4 SvcConfig
798 root S N 38M 542 1.2 31.4 SvcConfig
592 root S N 38M 542 1.2 31.4 SvcConfig
716 root S N 38M 542 0.8 31.4 SvcConfig
740 root S N 22M 589 0.4 18.7 PhoneletLaunche
591 root S N 38M 542 0.2 31.4 SvcConfig
590 root S N 38M 542 0.2 31.4 SvcConfig
556 root S N 38M 542 0.2 31.4 SvcConfig
666 root S N 38M 542 0.1 31.4 SvcConfig
545 root S N 38M 542 0.1 31.4 SvcConfig
9380 root R < 720 5660 0.1 0.5 menu_tree.cmd
543 root S < 38M 542 0.0 31.4 SvcConfig
594 root S N 38M 542 0.0 31.4 SvcConfig
748 root S N 38M 542 0.0 31.4 SvcConfig
751 root S N 38M 542 0.0 31.4 SvcConfig
749 root S N 38M 542 0.0 31.4 SvcConfig
856 root S N 38M 542 0.0 31.4 SvcConfig
593 root S N 38M 542 0.0 31.4 SvcConfig

3.17.5 Fault Trace Configuration

Error tracing and logging can be configured separately for all components, i. e. the services and applications running on the OpenStage phone. The resulting files can be viewed in the WBM web pages over the **Download** links.

The **File size (bytes)** parameter sets the maximum file size. When the maximum size is reached, the file is deleted, and a new file is generated. The trace data is then written to the new file. The default value is 65536.

The **Trace timeout (minutes)** determines when to stop tracing, i. e. writing to the trace file.

If **Automatic clear before start** is checked, the existing trace file will be deleted on pressing the **Submit** button, and a new, empty trace file will be generated. By default, it is unchecked.

You can read the log files by clicking on the appropriate hyperlinks (the hyperlinks work only if the file in question has been created). The following logs can be viewed:

- **Download trace file**
  The trace data according to the settings specified for the services.
- **Download boot file**
  The system messages of the booting process.
- **Download saved trace file**
  Normally, the trace file is saved only in the phone RAM. When the phone restarts in a controlled manner, the trace file will be saved in permanent memory.
- **Download saved boot file**
  Normally, the boot file is saved only in the phone RAM. When the phone restarts in a controlled manner, the boot file will be saved in permanent memory..
- **Download upgrade trace file**
  The trace log created during a software upgrade.
- **Download upgrade error file**
  The error messages created during a software upgrade.
- **Download exception file**
  If an exceptions occurs in a process running on the phone, a message is written to this file.
- **Download old exception file**
  The exception file is stored permanent memory. When the file has reached its size limit, it will be saved as old exception file, and the current exception file is emptied for future messages. The old exception file can be viewed here.
- **Download old trace file**
  The trace file is stored permanent memory. When the file has reached its size limit, it will be saved as old trace file, and the current exception file is emptied for future messages. The old trace file can be viewed here.
- **Download error file**

- **Download syslog file**

By pressing **Submit**, the trace settings are submitted to the phone. With **Reset**, the recent changes can be canceled.

The following trace levels can be selected:

- **OFF**: Default value. Only error messages are stored.
- **ERROR**: Error messages are stored.
- **TRACE**: Trace messages are stored. These contain detailed information about the processes taking place in the phone.
- **DEBUG**: All types of messages are stored.

Brief Descriptions of the Components/Services

- **Administration**
  Deals with the changing and setting of parameters within the phone database, from both the User and Admin menus.
- **Application framework**
  All applications within the phone, e.g. Call view, Call log or Phonebook, are run within the application framework. It is responsible for the switching between different applications and bringing them into and out of focus as appropriate.
- **Application menu**
  This is where applications to be run on the phone can be started and stopped.
- **Bluetooth service**
  Handles the Bluetooth interactions between external Bluetooth devices and the phone.
  Bluetooth is available only on OpenStage 60/80 phones.
- **Call log**
  The Call log application displays the call history of the phone.
- **Call view**
  Handles the representation of telephony calls on the phone screen.
- **Certificate management**
  Handles the verification and exchange of certificates for security and verification purposes.
- **Communications**
  Involved in the passing of call related information and signaling to and from the CSTA service.
- **Component registrar**
  Handles data relating to the type of phone, e.g. OpenStage 20/40 HFA/SIP, OpenStage 60/80 HFA/SIP.
- **CSTA service**

Any CSTA messages are handled by this service. CSTA messages are used within the phone by all services as a common call progression and control protocol.

- **Data Access service**
  Allows other services to access the data held within the phone database.
- **Desktop**
  Responsible for the shared parts of the phone display. Primarily these are the status bar at the top of the screen and the FPK labels.
- **Digit analysis service**
  Analyses and modifies digit streams which are sent to and received by the phone, e.g. canonical conversion.
- **Directory service**
  Performs a look up for data in the phonebook, trying to match incoming and outgoing numbers with entries in the phonebook.
- **DLS client management**
  Handles interactions with the DLS (Deployment Service).
- **Health service**
  Monitors other components of the phone for diagnostic purposes and provides a logging interface for the services in the phone.
- **Help**
  Handles the help function.
- **Instrumentation service**
  Used by the Husim phone tester to exchange data with the phone for remote control, testing and monitoring purposes.
- **Java**
  Any Java applications running on the phone will be run in the Java sandbox controlled by the Java service.
- **Journal service**
  Responsible for saving and retrieving call history information, which is used by the Call log application.
- **Media control service**
  Provides the control of media streams (voice, tones, ringing etc.) within the phone.
- **Media processing service**
  This is a layer of software between the media control service, the tone generation, and voice engine services. It is also involved in the switching of audio devices such as the handset and loudspeaker.
- **Mobility service**
  Handles the mobility feature whereby users can log onto different phones and have them configured to their own profile.
- **OBEX service**
  Involved with Bluetooth accesses to the phone.

Bluetooth is available only on OpenStage 60/80 phones.

- **Openstage client management**
  Provides a means by which other services within the phone can interact with the database.
- **Phonebook**
  Responsible for the phonebook application.
- **POT service**
  Takes over control of basic telephony if the callview application fails.
- **Password management service**
  Verifies passwords used in the phone.
- **Physical interface service**
  Handles any interactions with the phone via the keypad, mode keys, fixed feature buttons, clickwheel and slider.
- **Service framework**
  This is the environment within which other phone services operate. It is involved in the starting and stopping of services.
- **Service registry**
  Keeps a record of all services currently running inside the phone.
- **SIP call control**
  Contains the call model for the phone and is associated with telephony and call handling.
- **SIP messages**
  Traces the SIP messages exchanged by the phone.

After changing the level for the tracing of SIP messages, the phone must be rebooted. Otherwise the changes would have no effect.

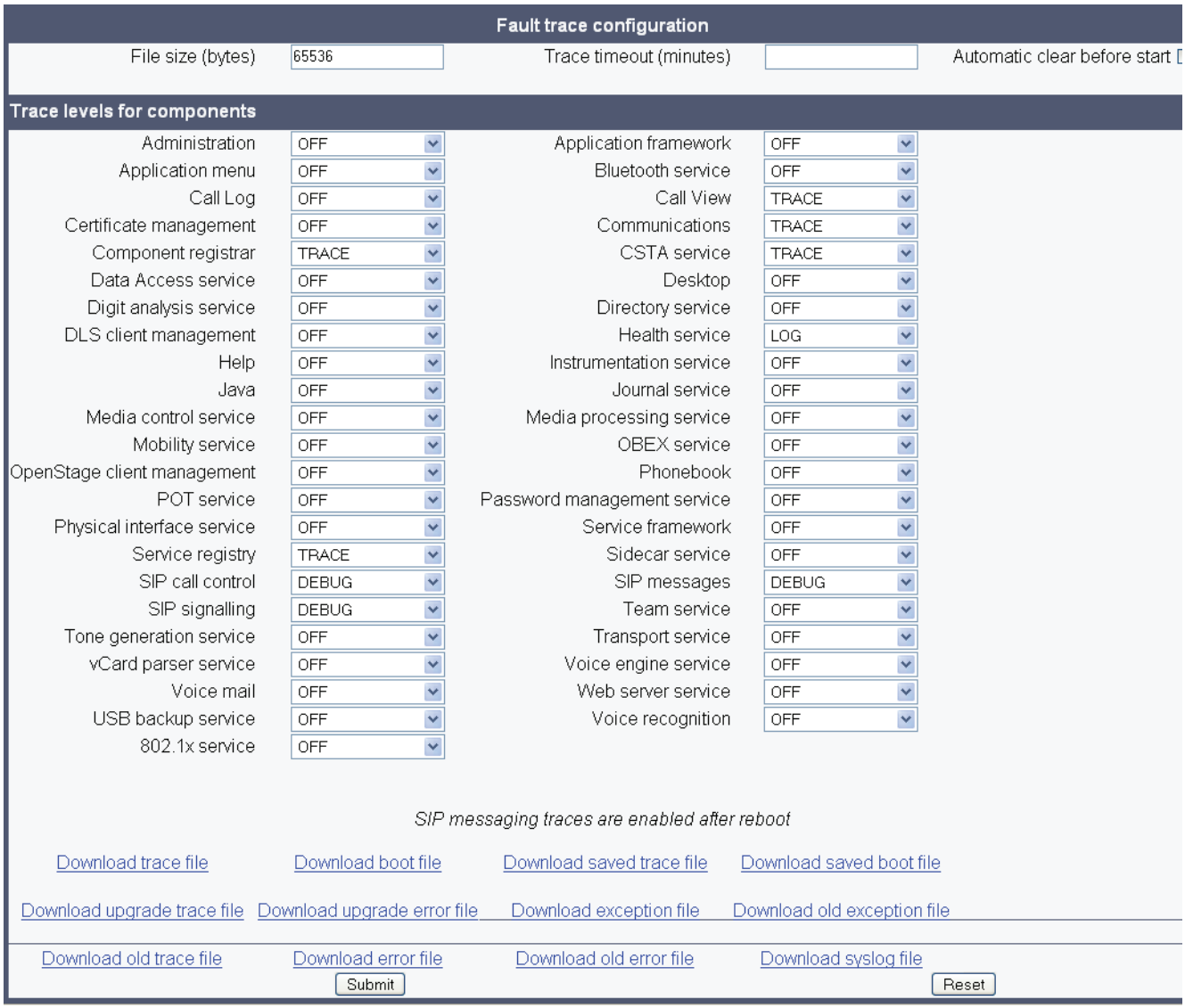
- **SIP signalling**
  Involved in the creation and parsing of SIP messages. This service communicates directly with the SIP stack.
- **Sidecar service**
  Handles interactions between the phone and any attached sidecars.
- **Team Service**
  Primarily concerned with keyset operation.
- **Tone generation service**
  Handles the generation of the tones and ringers on the phone.
- **Transport service**
  Provides the IP (LAN) interface between the phone and the outside world.
- **USB backup service (V1R3.x upwards)**
  Used to make backup/restore to/from USB stick by using password. This item is available in the phone GUI.
- **vCard parser service (V1R3.x upwards)**

Handles parsing and identification of VCard information while sending or getting VCards via Bluetooth.

- **Voice engine**
  Provides a switching mechanism for voice streams within the phone. This component is also involved in QDC, Music on hold and voice instrumentation.
- **Voice mail**
  Handles the voice mail functionality.
- **Voice recognition (V1R3.x upwards)**
  Used by the voice dial facility for recognizing spoken dialing commands.
- **Web Server service**
  Provides access to the phone via web browser.
- **802.1x service (V1R3.x upwards)**
  Provides authentication to devices attached to a LAN port, establishing a point-to-point connection or preventing access from that port if authentication fails. The service is used for certain closed wireless access points,

Administration via WBM

Diagnostics > Fault Trace Configuration



3.17.6 Easy Trace Profiles

In order to simplify tracing for a specific problem, the tracing levels can be adjusted using pre-defined settings. The Easy Trace profiles provide settings for a specific area, e. g. call connection. On pressing **Submit**, those pre-defined settings are sent to the phone. If desired, the settings can be modified anytime using the general mask for trace configuration under **Diagnostics** > Fault Trace Configuration (see Section 3.17.5, “Fault Trace Configuration”).

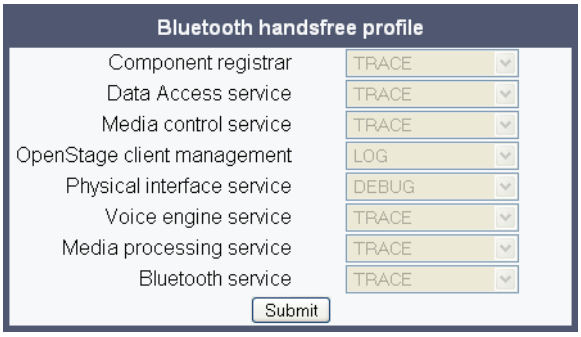
If desired, the tracing for all services can be disabled (see Section 3.17.6.23, “No Tracing for All Services”).

The following sections describe the Easy Trace profiles available for the phone.

3.17.6.1 Bluetooth Handsfree

Administration via WBM

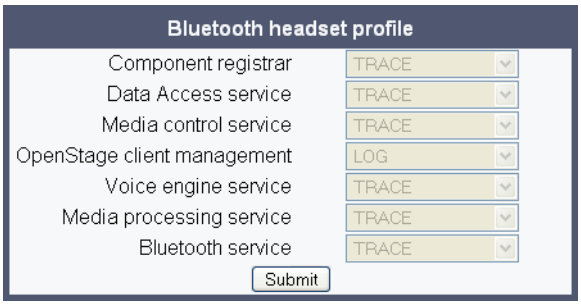
Diagnostics > Easy Trace Profiles > Bluetooth handsfree profile



3.17.6.2 Bluetooth Headset

Administration via WBM

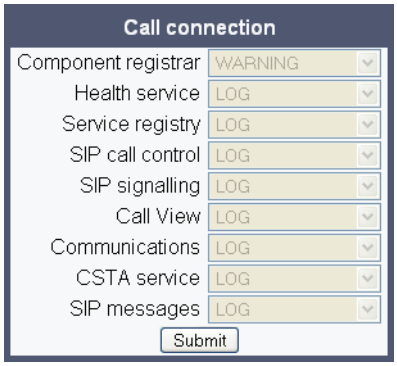
Diagnostics > Easy Trace Profiles > Bluetooth headset profile



3.17.6.3 Call Connection

Administration via WBM

Diagnostics > Easy Trace Profiles > Call connection

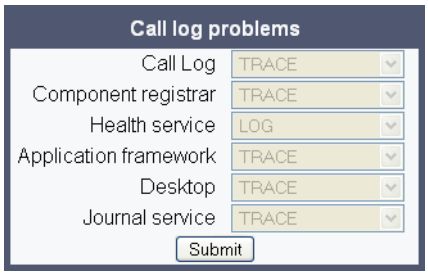


This Easy Trace profile contains the tracing of SIP messages. Please note that after changing the level for the tracing of SIP messages, the phone must be rebooted.

3.17.6.4 Call Log

Administration via WBM

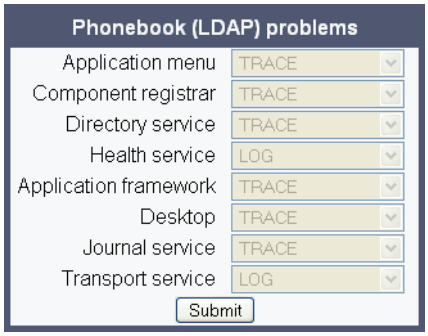
Diagnostics > Easy Trace Profiles > Call log problems



3.17.6.5 LDAP Phonebook

Administration via WBM

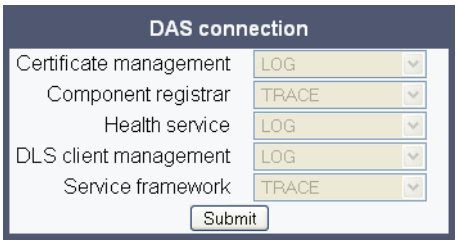
Diagnostics > Easy Trace Profiles > Phonebook (LDAP) problems



3.17.6.6 DAS Connection

Administration via WBM

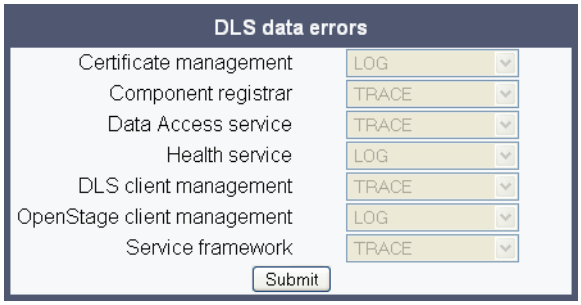
Diagnostics > Easy Trace Profiles > DAS connection



3.17.6.7 DLS Data Errors

Administration via WBM

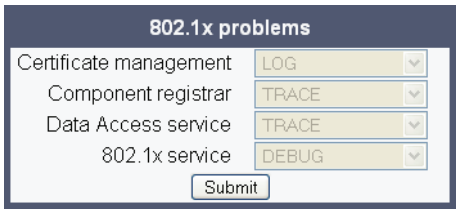
Diagnostics > Easy Trace Profiles > DLS data errors



3.17.6.8 802.1x

Administration via WBM

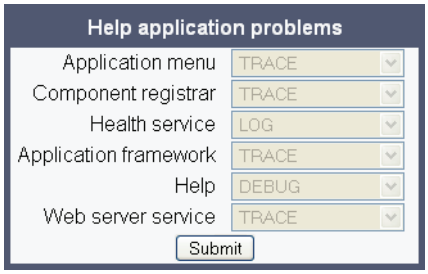
Diagnostics > Easy Trace Profiles > 802.1x



3.17.6.9 Help Application

Administration via WBM

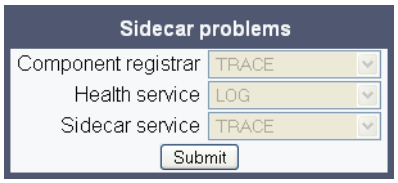
Diagnostics > Easy Trace Profiles > Help application problems



3.17.6.10 Sidecar

Administration via WBM

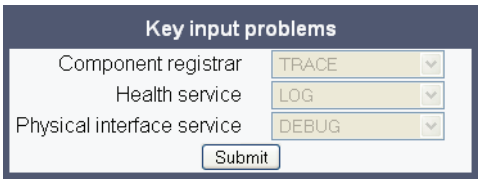
Diagnostics > Easy Trace Profiles > Sidecar problems



3.17.6.11 Key Input

Administration via WBM

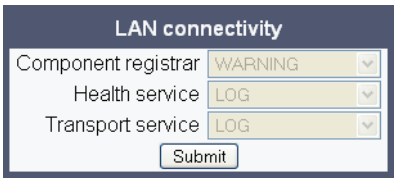
Diagnostics > Easy Trace Profiles > Key input problems



3.17.6.12 LAN Connectivity

Administration via WBM

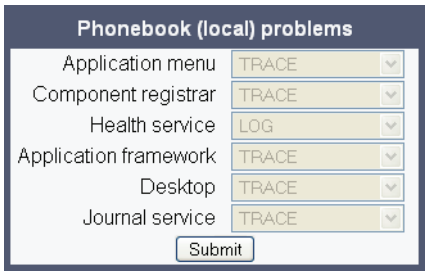
Diagnostics > Easy Trace Profiles > LAN connectivity problems



3.17.6.13 Local Phonebook

Administration via WBM

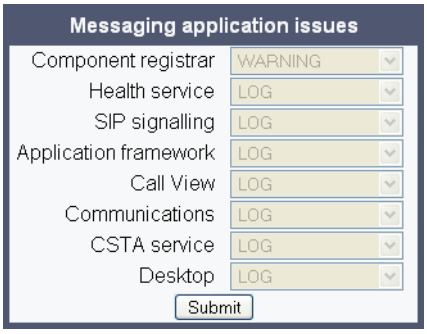
Diagnostics > Easy Trace Profiles > Phonebook (local) problems



3.17.6.14 Messaging

Administration via WBM

Diagnostics > Easy Trace Profiles > Messaging application problems



3.17.6.15 Mobility

Diagnostics > Easy Trace Profiles > Mobility problems

3.17.6.16 Phone administration

Diagnostics > Easy Trace Profiles > Phone administration problems

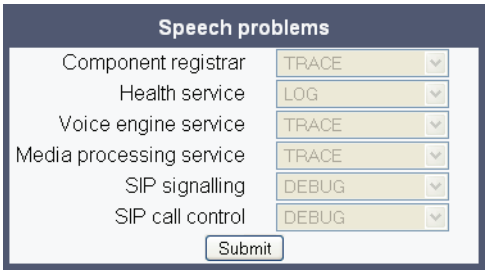
3.17.6.17 Server based applications

Diagnostics > Easy Trace Profiles > Server based application problems

3.17.6.18 Speech

Administration via WBM

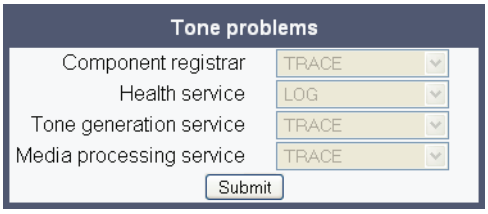
Diagnostics > Easy Trace Profiles > Speech problems



3.17.6.19 Tone

Administration via WBM

Diagnostics > Easy Trace Profiles > Tone problems



3.17.6.20 USB Backup/Restore

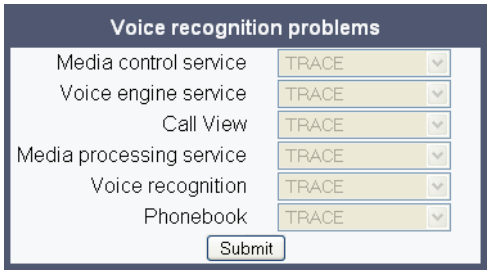
Administration via WBM

Diagnostics > Easy Trace Profiles > USB backup/restore

3.17.6.21 Voice Dialling

Administration via WBM

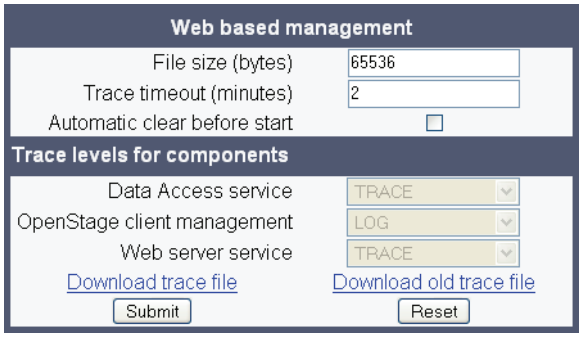
Diagnostics > Easy Trace Profiles > Voice recognition problems



3.17.6.22 Web Based Management

Administration via WBM

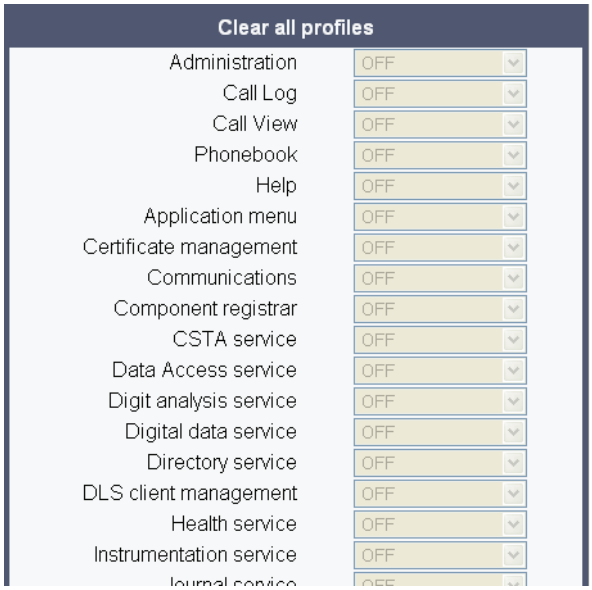
Diagnostics > Easy Trace Profiles > Web based management



3.17.6.23 No Tracing for All Services

Administration via WBM

Diagnostics > Easy Trace Profiles > Clear all profiles



3.17.7 QoS Reports

3.17.7.1 Conditions and Thresholds for Report Generation

For details about the functionality, please refer to the release notes.

The generation of QoS (Quality of Service) reports which are sent to a QCU server (see Section 3.3.8, “SNMP”) is configured here.

Data required

- **Report mode**: Sets the conditions for generating a QoS report.
  Value range:
  - "OFF": No reports are generated.
  - "EOS Threshold exceeded": Default value. A report is created if a) a telephone conversation longer than the **Minimum session length** has just ended, and b) a threshold value has been exceeded during the conversation.
  - "EOR Threshold exceeded": A report is created if a) the report interval has just passed, and b) a threshold value has been exceeded during the observation interval.
  - "EOS (End of Session)": A report is created if a telephone conversation longer than the **Minimum session length** has just ended.
  - "EOR (End of Report Interval)": A report is created if the report interval has just passed.
- **Report interval (seconds)**: Time interval between the periodical observations.
  Default: 60.
- **Observation interval (seconds)**: During this time interval, the traffic is observed.
  Value: 10.
- **Minimum session length (100 millisecond units)**: When the Report mode is set to "EOS Threshold exceeded" or "EOS (End of Session)", a report can be created only if the duration of the conversation exceeds this value.
  Default: 20.
- **Maximum jitter (milliseconds)**: When the jitter exceeds this value, a report is generated.
  Default: 20.
- **Average round trip delay (milliseconds)**: When the average round trip time exceeds this value, a report is generated.
  Default: 100.

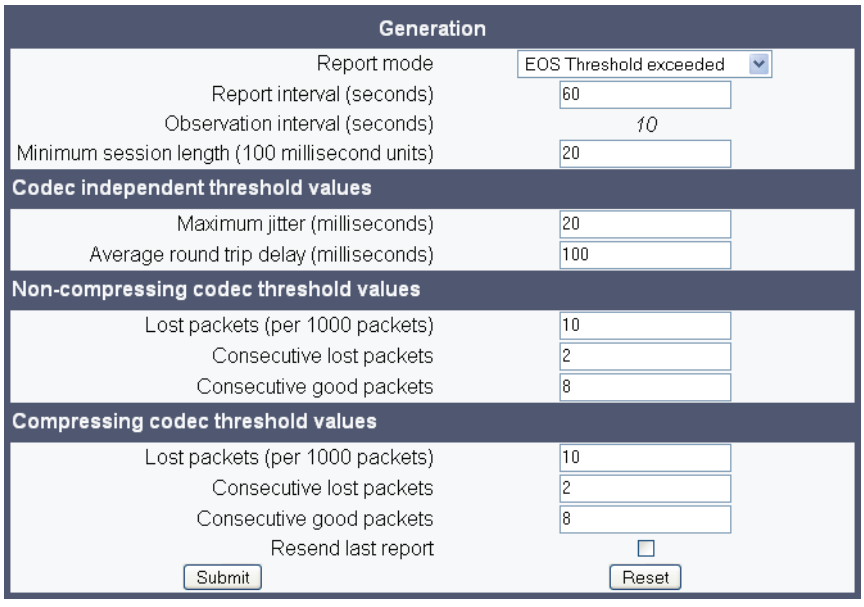
Non-compressing codecs / Compressing codes:

- **Lost packets (per 1000 packets)**: When the number of lost packets exceeds this maximum value during the observation interval, a report is created.
  Default: 10.
- **Consecutive lost packets**: When the number of lost packets following one another exceeds this maximum value during the observation interval, a report is created.
  Default: 2.
- **Consecutive good packets**: When the number of good packets following one another falls below this minimum value, a report is created.
  Default: 8.
- **Resend last report**: If checked, the previous report is sent once again on pressing **Submit**.
  Value range: "Yes", "No".
  Default: "No".

The transmission of report data can be triggered manually by pressing **Send now** in the local menu.

Administration via WBM

Diagnostics > QoS Reports > Generation



Administration via Local Phone

- Administration
  - Network
    - QoS
      - Reports
        - Generation
          - **Mode**
          - **Report interval**
          - **Observe interval**
          - **Minimum session length**
        - **Send now**
        - Thresholds
          - **Maximum jitter**
          - **Round-trip delay**
          - Non-compressing:
          - ...**Lost packets (K)**
          - ...**Lost consecutive**
          - ...**Good consecutive**
          - Compressing:
          - ...**Lost packets (K)**
          - ...**Lost consecutive**
          - ...**Good consecutive**

3.17.7.2 View Report

OpenStage phones generate QoS reports using a HiPath specific format, QDC (**Q**oS **D**ata **C**ollection). The reports created for the last 6 sessions, i. e. conversations, can be viewed on the WBM.

To enable the generation of reports, please ensure that:

- the switch **QoS traps to QCU** (System > SNMP) is activated (see Section 3.3.8, “SNMP”);
- the conditions for the generation of reports are set adequately (see Section 3.17.7.1, “Conditions and Thresholds for Report Generation”).

For details about QoS reports on HiPath devices, see the HiPath QoS Data Collection V 1.0 Service Manual.

A QoS report contains the following data:

- **Start of report period - seconds**: NTP time in seconds for the start of the report period.
- **Start of report period - fraction of seconds**: Additional split seconds to be added to the seconds for an exact start time.
- **End of report period - seconds**: NTP time in seconds for the end of the report period.
- **End of report period - fraction of seconds**: Additional split seconds to be added to the seconds for an exact end time.
- **SNMP specific trap type**: The trap type is a 5 bit value calculated from a list of threshold-exceeding bits. Every time a threshold is exceeded, the associated bit is set, otherwise it is cleared.
  The trace type bits are defined as follows:
  - Bit 0: Jitter threshold was exceeded.
  - Bit 1: Delay threshold was exceeded.
  - Bit 2: Threshold for lost packets was exceeded.
  - Bit 3: Threshold for consecutive lost packets was exceeded.
  - Bit 4: Threshold for consecutive good packets was exceeded.
- **IP address (local)**: IP address of the local phone.
- **Port number (local)**: RTP receiving port of the local phone.
- **IP address (remote)**: IP address of the remote phone that took part in the session.
- **Port number (remote)**: RTP sending port of the local phone.
- **SSRC (receiving)**: RTP Source Synchronization Identifier of the local phone.
- **SSRC (sending)**: RTP Source Synchronization Identifier of the remote phone.
- **Codec**: Number of the Payload Type applied in the session; see RFC 3551 (Table 4 and 5).
- **Maximum packet size**: Maximum size (in ms) of packets received during the report interval.

- **Silence suppression**: Number of silence suppression activation objects found in the RTP stream received. A silence suppression activation object is defined as a period of silence when no encoded voice signals were transmitted by the sender.
- **Count of good packets**: Total amount of good packets.
- **Maximum jitter**: Maximum jitter (in ms) found during the report interval.
- **Maximum inter-arrival jitter**: Maximum of the interarrival jitter values (in ms). The interarrival jitter is the smoothed absolute value of the jitter measurements. It is calculated continuously. For details about the calulation, see RFC 3550.
- **Periods jitter threshold exceeded**: Number of observation intervals in which the threshold for maximum jitter was exceeded.
- **Round trip delay**: Average value of delay calculated for each RTCP packet. The first value is available after about 15 sec.
- **Round trip delay threshold exceeded**: Set to "true" if the average round trip delay threshold value was exceeded in the report interval.
- **Count of lost packets**: Number of packets lost in the course of speech decoding.
- **Count of discarded packets**: Number of the packets discarded without transferring the contents.
- **Periods of lost packets**: Number of observation intervals in which the threshold for lost packets was exceeded.
- **Consecutive packet loss (CPL)**: List of sequences consecutive packets that were all lost, grouped according to the amount of packets per sequence. The first number in the list counts single lost packets, the second number counts sequences of two lost packets, and so on. The last number counts sequences of more than 10 lost packets.
- **Periods of consecutive lost packets**: Number of observation intervals in which the threshold for consecutive lost packets was exceeded.
- **Consecutive good packets (CGP)**: List of sequences consecutive packets that were all processed, grouped according to the amount of packets per sequence. The first number in the list counts single good packets, the second number counts sequences of two good packets, and so on. The last number counts sequences of more than 10 good packets. All values are reset to 0 after an interval without packet loss.
- **Periods of consecutive good packets**: Number of intervals in which the count of lost packets went below the threshold.
- **Count of jitter buffer overruns**: Number of packets rejected because the jitter buffer was full.
- **Count of jitter buffer under-runs**: Increased by one whenever the decoder requests new information on decoding and finds an empty jitter buffer.
- **Codec change on the fly**: The value is 1, if there has been a codec or SSRC change during the observation period, and 0, if there has been no change.
- **Periods with at least one threshold exceeded**: Number of observation intervals with at least one threshold exceedance. If there is no data, the value is 255. The threshold values included are:

  - maximum jitter;
  - lost packets;
  - consecutive lost packets;
  - consecutive good packets.
- **HiPath Switch ID**: Unique number identifying the HiPath switch to which the endpoints are assigned.
- **LTU number**: In HiPath 4000 only, the shelf identification is taken from the shelf containing a gateway.
- **Slot number**: The slot number where the phoneis connected in the shelf.
- **Endpoint type**: Type of the local phone.
- **Version**: Software version of the local phone.
- **Subscriber number type**: Type of subscriber number assigned to the local phone. The possible types are:
  - 1: local number, extension only;
  - 2: called number, network call
  - 3: E.164 number of the local phone.
- **Subscriber number**: Subscriber number of the local phone.
- **Call ID**: SIP call id.
- **MAC address**: MAC address of the local phone.

Data viewing via WBM:

Diagnostics > QoS reports > View Session Data

View Session Data

Select a report to view	QoS Statistics 1
Submit	
Start of report period - seconds	3394450938
Start of report period - fraction of seconds	31669
End of report period - seconds	3394451013
End of report period - fraction of seconds	17820
SNMP specific trap type	0
IP address (local)	192.168.1.12
Port number (local)	5004
IP address (remote)	192.168.1.15
Port number (remote)	5010
SSRC (receiving)	324951319
SSRC (sending)	1987331861
Codec	0
Maximum packet size	20
Silence suppression	0
Count of good packets	3638
Maximum jitter	4
Maximum inter-arrival jitter	2
Periods jitter threshold exceeded	0
Round trip delay	2
Round trip delay threshold exceeded	☐
Count of lost packets	0
Count of discarded packets	0
Periods of lost packets	0
Consecutive packet loss (CPL)	255,255,255,255,255,255,255,255,255,255,255
Periods of consecutive lost packets	255
Consecutive good packets (CGP)	255,255,255,255,255,255,255,255,255,255,255
Periods of consecutive good packets	255
Count of jitter buffer overruns	0
Count of jitter buffer under-runs	0
Codec change on the fly	☐
Periods with at least one threshold exceeded	0
HiPath Switch ID	Unknown
LTU number	255
Slot number	255
Endpoint type	
Version	V1 R2.2.63 SIP 070629
Subscriber number type	0
Subscriber number	4711
Call ID	122384c56462fd0a6bfa22b6364005f3@192.168.1.21
MAC address	0001e3247e50

3.17.8 Core dump

If **Enable core dump** is checked, a core dump will be initiated in case of a severe error. The core dump will be saved to a file. By default, this function is activated.

When **File size unlimited** is checked, there is no size limit for the core dump file. By default, it is not checked.

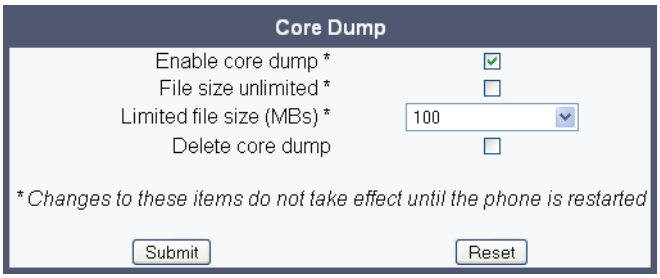
The maximum size for core dump files in MBytes can be chosen in the **Limited file size (MBs)** field. The possible values are 1, 5, 10, 25, 50, 75, and 100. The default value is 100.

If **Delete core dump** is activated, the current core dump file is deleted on **Submit**. By default, this is not activated.

If one or more core dump file exist, hyperlinks for downloading will be created automatically.

Administration via WBM

Diagnostics > Miscellaneous > Core dump



3.17.9 Remote Tracing - Syslog (V1R4.x upwards)

All trace messages created by the components of the phone software can be sent to a remote server using the syslog protocol. This is helpful especially for long-term observations with a greater number of phones.

To enable remote tracing, **Remote trace status** must be set to "Enabled". Furthermore, the IP address of the server receiving the syslog messages must be entered in **Remote ip**, and the corresponding server port must be given in **Remote port**.

Administration via Local Phone

- Administration
  - Maintenance
    - Remote trace
      - **Remote trace status**
      - **Remote ip**
      - **Remote port**

3.17.10 Test Interface

This parameters enables or disables the test interface (HPT).

Administration via WBM

Maintenance > Test interface

Administration via Local Phone

```
└--- Administration
     └--- Maintenance
          └--- Disable HPT
```

3.18 Bluetooth

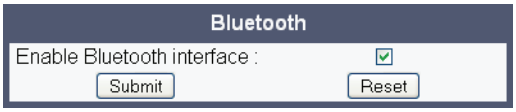
The Bluetooth interface can be enabled or disabled in the admin menu. By default, it is enabled. If Bluetooth is enabled, the user has the possibility to activate or deactivate it.

In version V1R3.x upwards, the Bluetooth address is displayed.

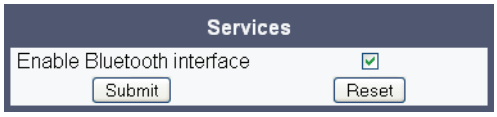
Bluetooth is available only on OpenStage 60/80 phones.

Administration via WBM

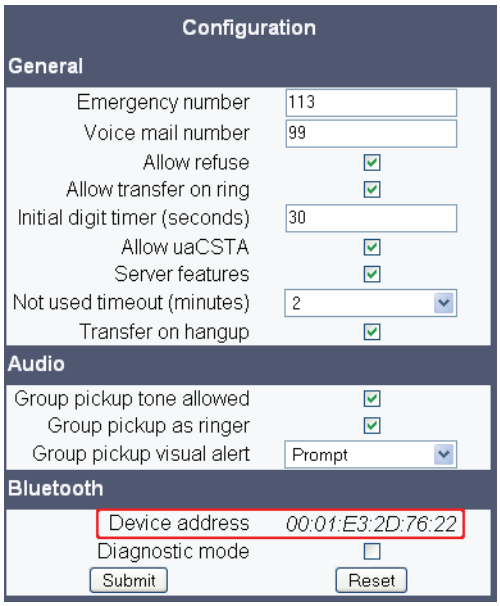
V1R2.x: Bluetooth



V1R3.x and upwards: System > Features > Feature access > Services



V1R4.x and upwards: System > Features > Configuration



Administration via Local Phone

In V1R2.x, only enabling or disabling Bluetooth is possible via the local admin menu:

└─ Administration

```
    |--- Bluetooth
        |--- Enable
```

In V1R3.x and upwards, only the device address can be viewed via the local admin menu:

```
|--- Administration
    |--- System
        |--- Features
            |--- Configuration
                |--- Bluetooth
                    |--- Local device address
```

4 Examples and HowTos

4.1 Canonical Dialing

4.1.1 Canonical Dialing Settings

The following example shows settings suitable for the conversion of given dial strings to canonical format. The example phone is located in Nottingham, UK.

Parameter	Example value	Explanation
Local country code	44	International country code for the UK.
National prefix digit	0	Used in front of national codes when dialled without international prefix.
Local national code	115	Area code within the UK (here: Nottingham).
Minimum local number length	7	Minimum number of digits in a local PSTN number (e. g. 3335333 = 7 digits).
Local enterprise node	780	Prefix to access Nottingham numbers from within the Siemens network.
PSTN access code	9	Prefix to make an international call in the UK.
Operator codes	0, 7800	Set of numbers to access the local operators.
Emergency numbers	999, 555	Set of numbers to access emergency services.
Initial extension digits	2, 3, 4, 5, 6, 8	1st digits of numbers that are used for extension numbers on the local node.

Tabelle 4-1

4.1.2 Canonical Dial Lookup

The following example shows settings suitable for recognizing incoming numbers and assigning them to entries in the local phone book, and for generating correct dial strings from phone book entries, depending on whether the number is internal or external.

Parameter	Example value	Explanation
Local code <1>	780	Enterprise node prefix (here: Nottingham).
International code <1>	+44115943	Equivalent prefix to access numbers on this node from the PSTN. Here, the prefix used by the PSTN (DID/DDI: direct inward dialing) is 943, which differs from the enterprise node prefix used within the enterprise network.
Local code <2>	722	Enterprise node prefix (here: Munich).
International code <2>	+4989722	Equivalent prefix to access numbers on this node from the PSTN. Here, the prefix used by the PSTN for direct inward dialing is identical to the enterprise node prefix.

4.1.2.1 Conversion examples

In the following examples, numbers entered into the local phonebook by the user are converted according to the settings given above.

Example 1: Internal number, same node as the local phone

User entry		2345
External numbers		Local public form
External access code		Not required
International gateway code		Use national code
Number stored in the phone book		+441159432345
Dial string sent when dialing from the phone book	Internal numbers = Local enterprise form	1234
	Internal numbers = Always add node	7802345
	Internal numbers = Use external numbers	9432345

Tabelle 4-2

Example 2: Internal number, different node

User entry		7222345
External numbers		Local public form
External access code		Not required
International gateway code		Use national code
Number stored in the phone book		+49897222345
Dial string sent when dialing from the phone book	Internal numbers = Local enterprise form	2345
	Internal numbers = Always add node	7802345
	Internal numbers = Use external numbers	9432345

Example 3: External number, same local national code as the local phone

User entry		011511234567
External numbers		Local public form
External access code		Not required
International gateway code		Use national code
Number stored in the phone book		+4411511234567
Dial string sent when dialing from the phone book	External numbers = Local public form	234567
	External numbers = National public form	011511234567
	External numbers = International form	004411511234567

4.2 How to Create Logo Files for OpenStage Phones

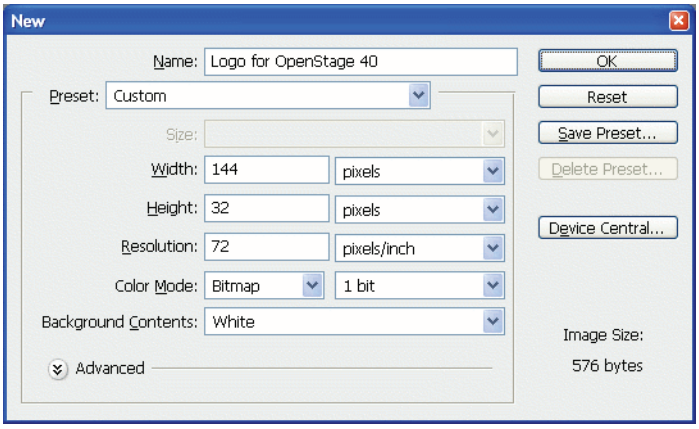
4.2.1 For OpenStage 40

1. Create a New Image

Create an image with the following specifications:

- Width: 144 px
- Height: 32 px
- Color Mode: 1 bit (monochrome)

Adobe Photoshop:



2. Insert the Logo

Place the logo image on the background, e.g. by copying it from a source file. Due to the size and color specifications, some adaptations may be necessary.

Adobe Photoshop Example:

3. Save the Image

Finally, save the image in BMP format. You can now upload the logo file to the phone as described in Section 3.10.7, “Logo”.

4.2.2 For OpenStage 60/80

In the following, the creation of a transparent image suitable for use as a logo in OpenStage 60/80 is described. This description is based on Adobe Photoshop, but any similar graphics software can be used as well.

Because of performance issues, half transparency in the alpha channel of the PNG files is not allowed on OpenStage phones. Therefore only 100% transparency or no transparency is used in the phone's UI elements.

1. Select the Background Color

For production purposes, we set the background color to the background color of the skin currently selected on the phone. Later, the background color will be replaced by transparency, which facilitates placing a logo on a gradient background. The following table lists the hexadecimal values, as used in HTML:

Phone Type	Skin	Color Code
OpenStage 60	Crystal Sea	#BDBDBD
OpenStage 60	Warm Grey	#424242[1]
OpenStage 80	Crystal Sea	#E6EBEF
OpenStage 80	Warm Grey	#3A3D3A

Tabelle 4-3

1 The background color on WP4 - skin 1 is a gradient; the colour listed here is an average value.

Adobe Photoshop:

Click on the Background Color icon on the Color palette group, then type the color code without leading "#" into the **#** field)

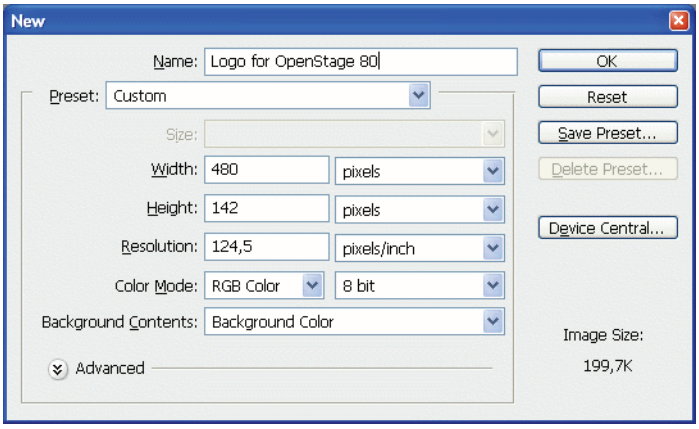
2. Create a New Image

Create an image with the size according to the phone type:

Phone Type	Size (px)
OpenStage 60	240 x 70
OpenStage 80	480 x 142

Tabelle 4-4

Adobe Photoshop:



3. Insert the Logo

Place the logo image on the background, e.g. by copying it from a source file.

Adobe Photoshop Example:

4. Merge Layers

Merge the two layers to one.

Adobe Photoshop:

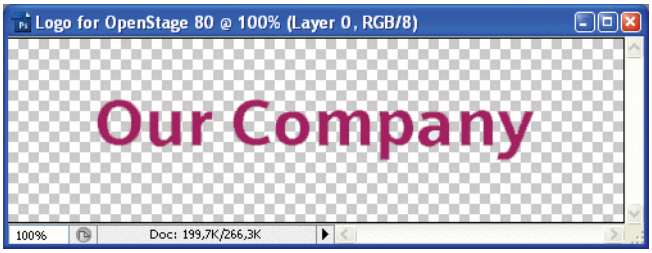
In the Panel, select both the background layer and the new layer containing the inserted logo. Afterwards, go to **Layer** in the Menu bar, and select **Merge Layers**.

5. Background Transparency

Delete the background colour so that only the exact former background colour is 100% transparent.

Adobe Photoshop:

Make sure that the background color is selected by clicking on the Background Color icon. In the Tool palette, click on the Eraser symbol with the right Mouse button and select the **Magic Eraser Tool**. After this, got to the Menu bar and set the **Tolerance** field to "0".



6. Save the Image

Finally, save the image in PNG format. You can now upload the logo file to the phone as described in Section 3.10.7, “Logo”.

4.3 How to Set Up the Corporate Phonebook (LDAP)

The Corporate Phonebook function is based on an LDAP client that can be connected to the company's LDAP service. A variety of LDAP servers can be used, for instance Microsoft Active Directory, OpenLDAP, or Apache Directory Server.

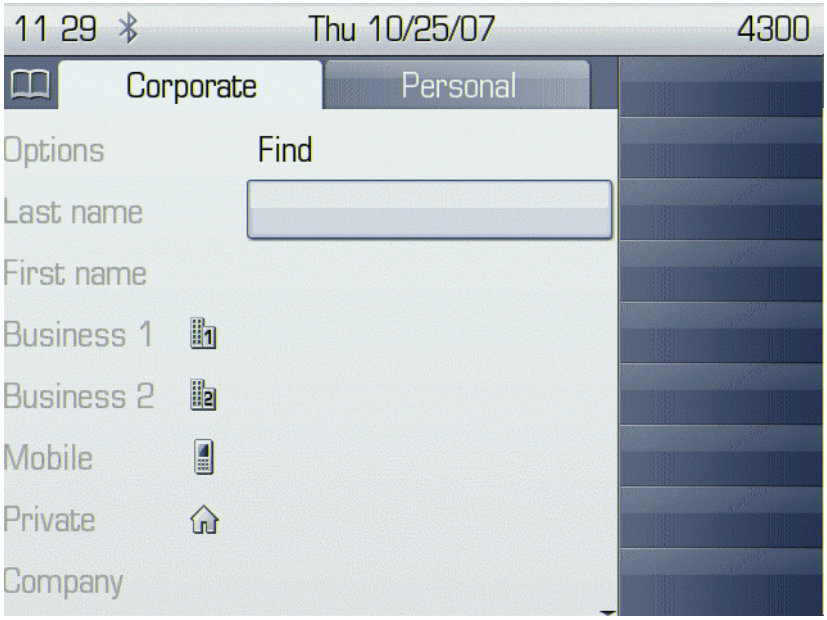
The Corporate Phonebook is available only on OpenStage 60/80.

4.3.1 Prerequisites:

1. An LDAP server is present and accessible to the phone's network. The standard port for LDAP is **389**.
2. Query access to the LDAP server must be provided. Unless anonymous access is used, a user name and passwort must be provided. It might be feasible to use a single login/password for all OpenStage phones.
3. To enable dialing internal numbers from the corporate phonebook, an LDAP entry must be provided that contains the proper number format required by the HiPath 8000.
   In Microsoft Active Directory, the standard LDAP attribute `telephoneNumber` is typically populated as follows: **+1<area code><call number>**. However, in a standard configuration, the HiPath 8000 will not handle this dial string correctly, due to the **+1** prefix. Therefore, it is recommended to use the **ipPhone** field, which is typically unused in Active Directory. It can be found in the **Telephones** tab of the Active Directory User Manager.

4.3.2 Create an LDAP Template

The user interface of the corporate phonebook application provides a form which is used both for search and retrieval.



The task of an LDAP template is to map the phone's search and display fields to LDAP attributes that can be delivered by the server. In the LDAP template, the fields are represented by hard-coded names: `ATTRIB01`, `ATTRIB02`, and so on. These field names are assigned to LDAP attributes, as appropriate.

The following examples show the relations between GUI field names, the attribute labels used in the template, and exemplary mappings to LDAP attributes.

Generic Example (Standard Attributes)

OpenStage Field	LDAP Template Lables	LDAP Attribute	Example Value
Last name	ATTRIB01	sn	Doe
First name	ATTRIB02	givenName	John
Business 1	ATTRIB03	telephoneNumber	9991234
Business 2	ATTRIB04	facsimileTelephoneNumber	9992345
Mobile	ATTRIB05	mobile	017711223344
Private	ATTRIB06	homePhone	441274333444
Company	ATTRIB07	o	Example Inc.
Address 1	ATTRIB08	departmentNumber	0815
Address 2	ATTRIB09		
Job function	ATTRIB10	title	Product Manager
Email	ATTRIB11	mail	doe@example.com

Given "example.com" as the LDAP subtree to be searched, the LDAP template file would look like this:

```
OpenStage LDAP TEMPLATE (v.1)
SEARCHBASE="dc=example,dc=com"
ATTRIB01="sn"
ATTRIB02="givenname"
ATTRIB03="telephoneNumber"
ATTRIB04="facsimileTelephoneNumber"
ATTRIB05="mobile"
ATTRIB06="homePhone"
ATTRIB07="o"
ATTRIB08="departmentNumber"
ATTRIB09=""
ATTRIB10="title"
ATTRIB11="mail"
EOF
```

Microsoft Active Directory Specific Example

OpenStage Field	LDAP Template Attribute	LDAP Attribute	Example Value
Last name	ATTRIB01	sn	Doe
First name	ATTRIB02	givenName	John
Business 1	ATTRIB03	ipPhone	9991234
Business 2	ATTRIB04	otherTelephone	9992345
Mobile	ATTRIB05	mobile	017711223344
Private	ATTRIB06	homePhone	441274333444
Company	ATTRIB07	company	Example Inc.
Address 1	ATTRIB08	department	Administration
Address 2	ATTRIB09		
Job function	ATTRIB10	title	Product Manager
Email	ATTRIB11	mail	doe@example.com

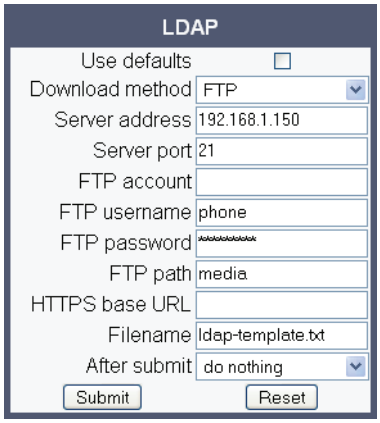
Given "example.com" as the LDAP subtree to be searched, the LDAP template file would look like this:

```
OpenStage LDAP TEMPLATE (v.1)
SEARCHBASE="dc=example,dc=com"
ATTRIB01="sn"
ATTRIB02="givenname"
ATTRIB03="ipPhone"
ATTRIB04="otherTelephone"
ATTRIB05="mobile"
ATTRIB06="homePhone"
ATTRIB07="company"
ATTRIB08="department"
ATTRIB09=""
ATTRIB10="title"
ATTRIB11="mail"
EOF
```

4.3.3 Load the LDAP Template into the Phone

When you have configured the LDAP template, you can upload it to the phone:

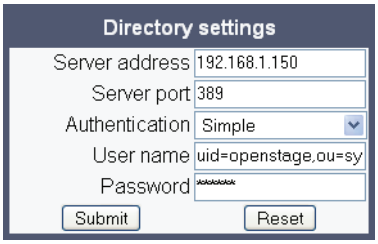
1. Save the template under a suitable name, for example, `ldap-template.txt`.
2. Copy the template file to the FTP server designated for deploying LDAP templates.
3. Upload the file using the WBM (see Section 3.10.6, “LDAP Template”), or, alternatively, the Local menu, or the DLS (see the Deployment Service Administration Manual). For an example configuration, see the following WBM screenshot (path: **File transfer** > LDAP):



4.3.4 Configure LDAP Access

To enter the access data using the WBM, take the following steps:

1. Navigate to **Local Functions** > Directory Settings.
2. Enter the following parameters:
   - **Server address** (IP address or hostname of the LDAP server)
   - **Server port** (port used by the LDAP, typically 389)
   - **Authentication** (authentication method for the connection to the LDAP server)
   - **User name** (only required if simple authentication is selected); **Password** (relating to the user name).



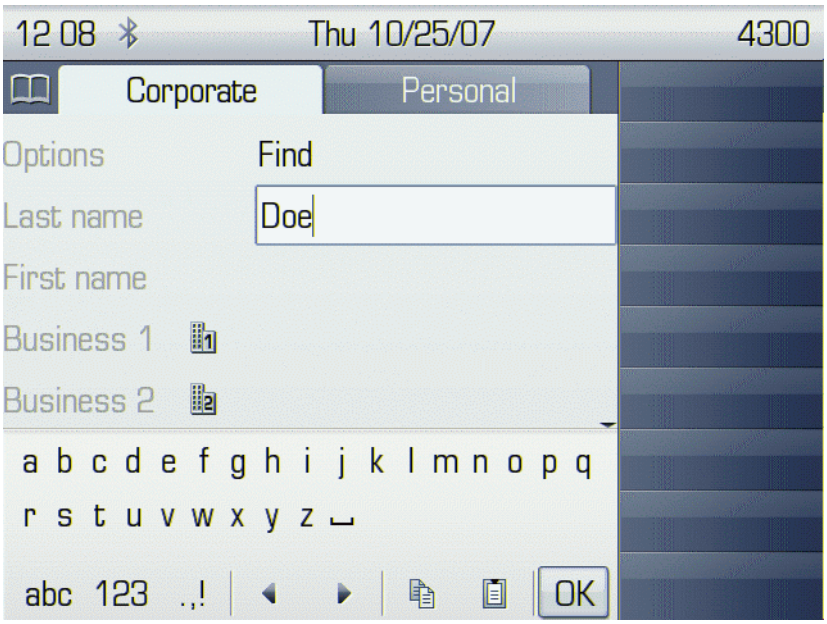
3. Press **Submit**.

4.3.5 Test

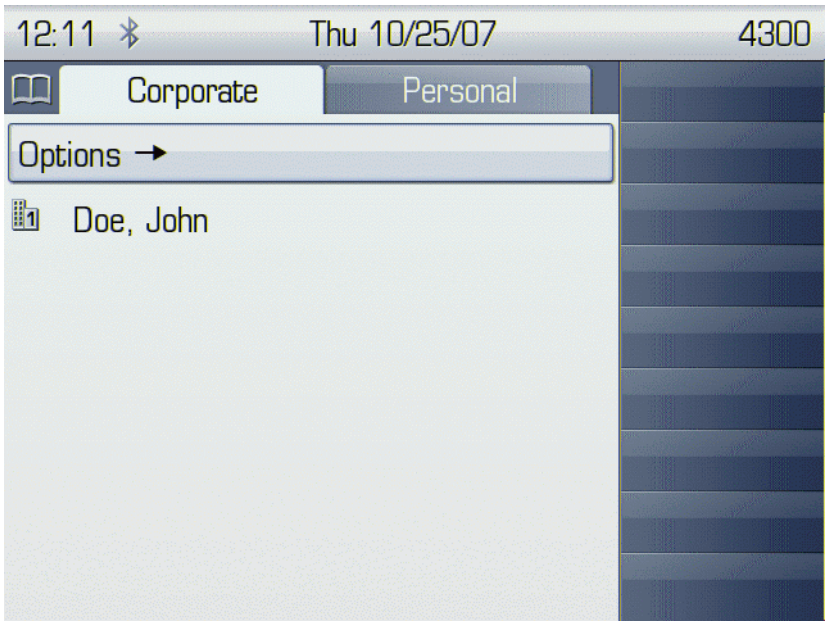
If everything went well, you can run a test query on your OpenStage phone.

1. To navigate to the phone's corporate phonebook, press the 📖 button twice.
2. Press ➔ on the TouchGuide. In the context menu, select Find by pressing OK.
3. In the query mask, select the entry to be searched, for instance **Last Name**. Press OK to open the onscreen keypad for text input.

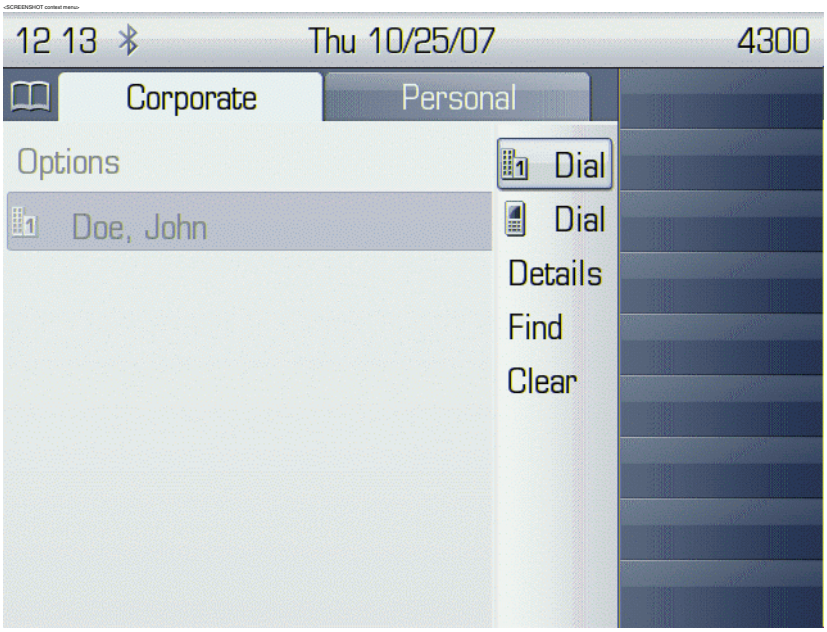
4. Enter the text to be searched. For information on using the onscreen keypad, see Section 3.1, “Access via Local Phone”, step 5.



6. Navigate to the Find option and press OK. If the query was successful, at least one entry will be listed in the following manner:



7. Navigate to the desired entry and press ➔ on the TouchGuide to open the context menu. You can select one of the following options:
   - Dial the **Business 1** number.
   - Dial the **Mobile** number.
   - Have the entry's details, that is, all attributes displayed.
   - Start a new search.
   - Clear the list of search results.



5 Technical Reference

5.1 Menus

This section describes the structure of the administration menus of the OpenStage phone. For information on user menus, please refer to the user manual.

5.1.1 Web Interface Menu

5.1.1.1 Menu Structure

Admin Login

Applications

- **XML applications**[1]
  - Add application
  - Modify application
  - Xpressions

Bluetooth[1] [2]

Network

- IP configuration (V1R2.x) / IP configuration (V1R3.x upwards)
- Update Service (DLS)
- QoS
- Port configuration (V1R2.x and V1R3.x on OpenStage 20/40) / Port configuration (V1R3.x upwards on OpenStage 60/80)

System

- System Identity
- SIP interface (V1R2.x) / SIP interface (V1R3.x)
- Registration
- SNMP
- **Features**
  - Configuration (V1R2.x) / Configuration (V1R3.x upwards on OpenStage 20/40) / Configuration (V1R3.x upwards on OpenStage 60/80)
  - DSS settings[3]

1. OpenStage 60/80 only.
2. In V1R3.x upwards, this parameter has moved to System > Features >
3. OpenStage 40/60/80 only.

- Program keys > Line[2]
- Key Module 1[2]
- Key Module 2[2]
- Keyset operation[2]
- Services
- **Feature access**[1]
  - Services (V1R3.x)
- Security (V1R4.x)

File transfer

- Defaults
- Phone application
- Hold music
- Picture Clip[1]
- LDAP[1]
- Logo[3]
- Screensaver[1]
- Ringer file
- Dongle key

Local functions

- Directory settings[1]
- **Locality**
  - Canonical dial settings
  - Canonical dial lookup
  - Canonical dial
- Pixel Saver (V1R4.x)

Date and time

Speech

- Codec preferences
- Audio settings

General information

Authentication

- Change Admin password
- Change User password

Diagnostics

- Fault trace configuration
- **EasyTrace Profiles**

- Bluetooth handsfree profile[1]
- Bluetooth headset profile[1]
- Call connection
- Call log problems
- DAS connection
- DLS data errors
- Help application problems[1]
- Key input problems
- LAN connectivity problems
- Messaging application problems
- Mobility problems
- Phone administration problems
- Phonebook (LDAP) problems[1]
- Phonebook (local) problems[1]
- Server based application problems[1]
- Sidecar problems
- Speech problems
- Tone problems
- USB backup/restore[1]
- Voice recognition problems[1]
- Web based management
- 802.1x problems
- Clear all profiles

QoS Reports

- Generation
- View Session Data

Miscellaneous

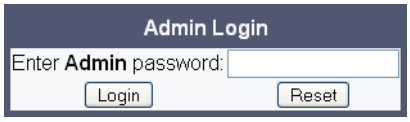
- IP tests
- Memory information
- Core dump

Maintenance

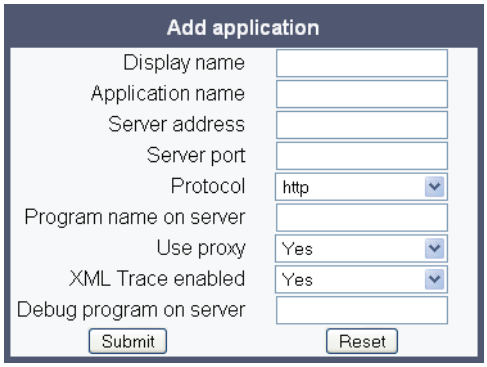
- Remote trace (V1R4.x upwards)
- Restart phone
- Factory reset
- HPT interface

5.1.1.2 Web Pages

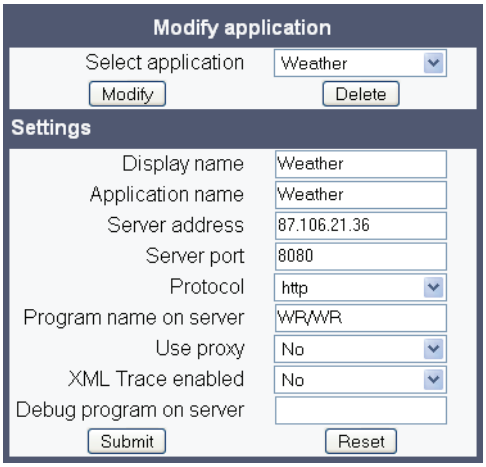
Admin Login



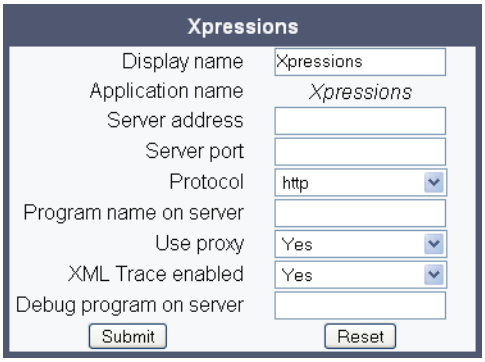
Add application



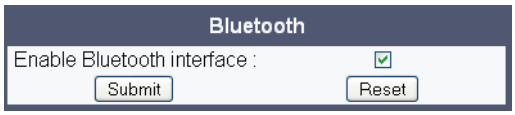
Modify application



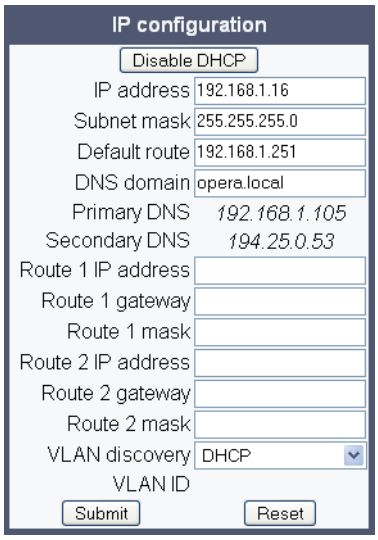
Xpressions



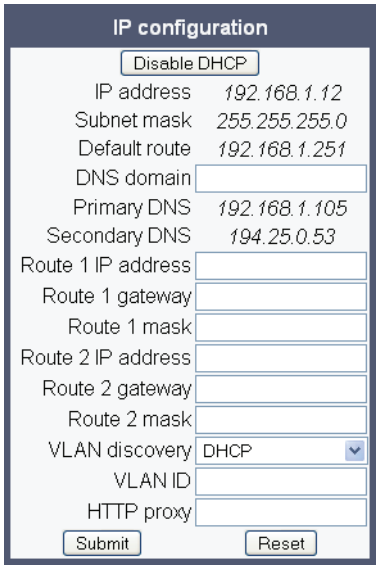
Bluetooth



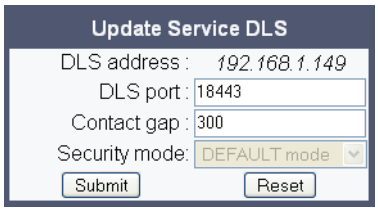
IP configuration (V1R2.x)



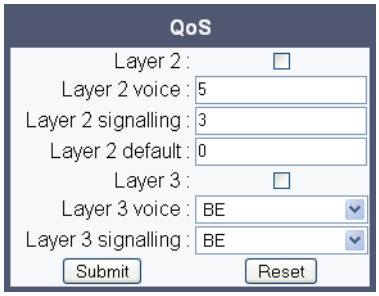
IP configuration (V1R3.x upwards)



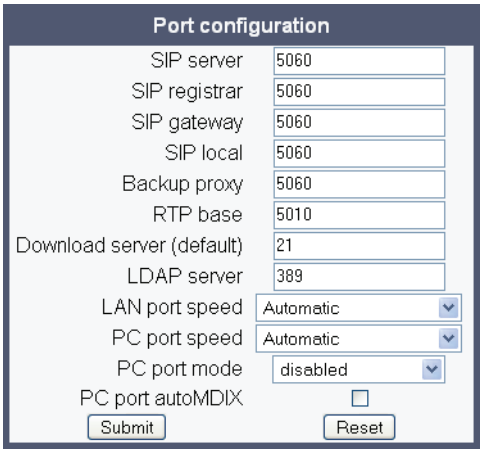
Update Service (DLS)



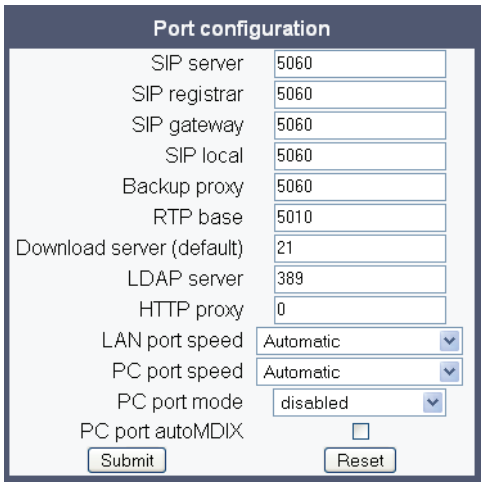
QoS



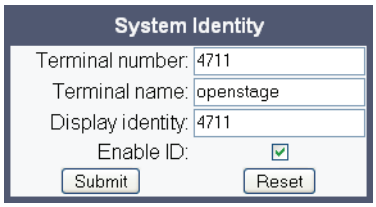
Port configuration (V1R2.x and V1R3.x on OpenStage 20/40)



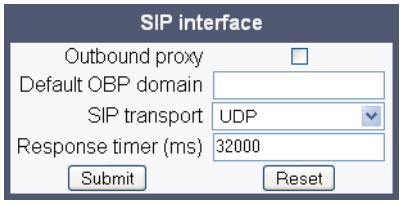
Port configuration (V1R3.x upwards on OpenStage 60/80)



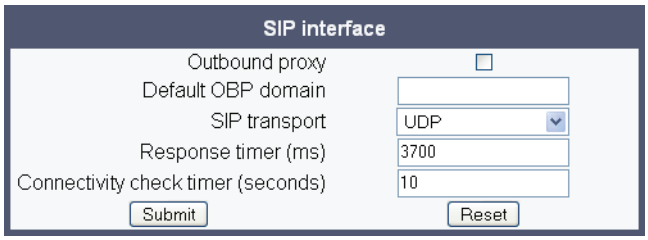
System Identity



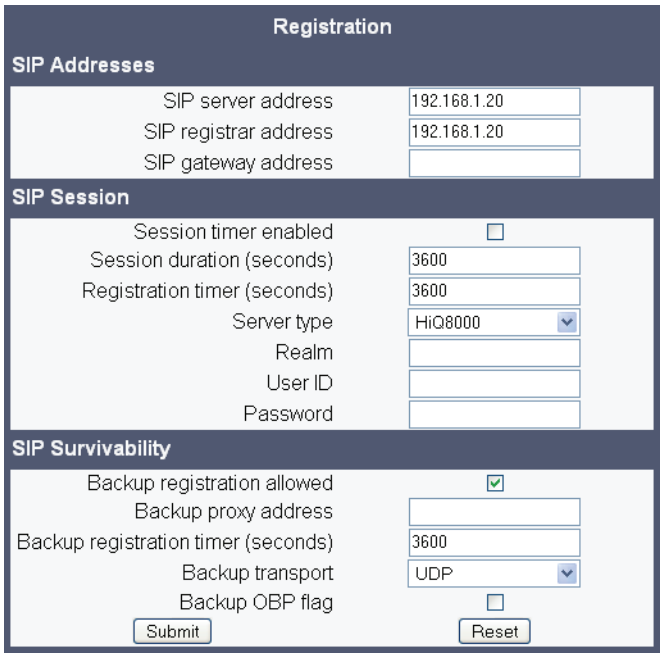
SIP interface (V1R2.x)



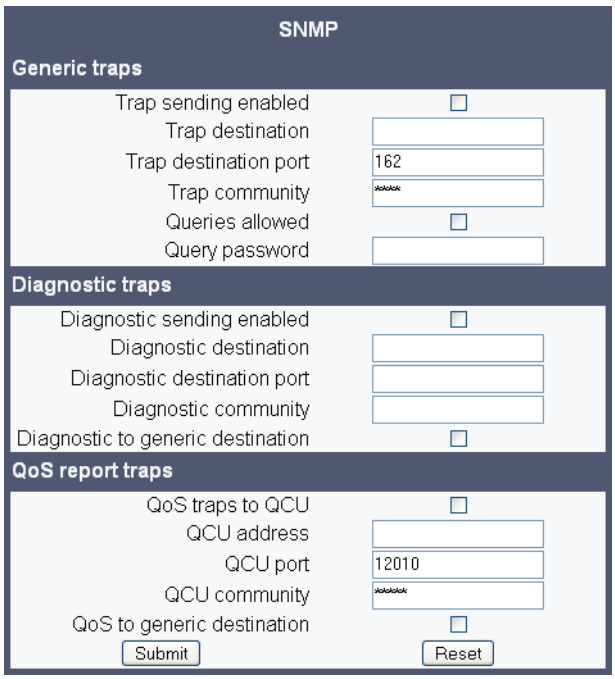
SIP interface (V1R3.x)



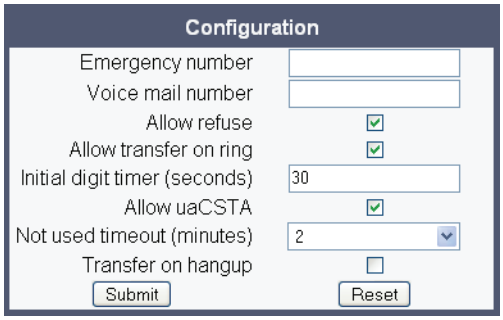
Registration



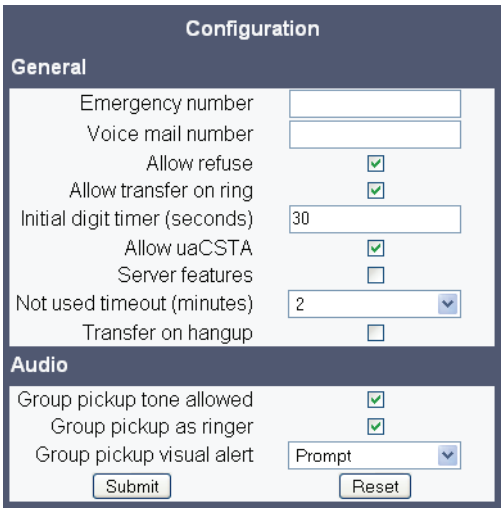
SNMP



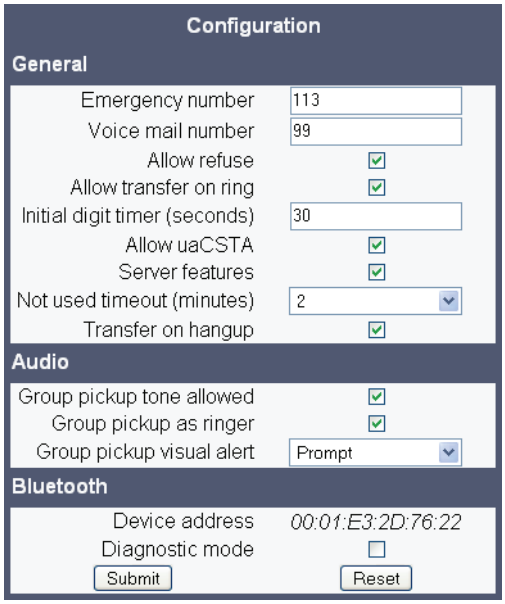
Configuration (V1R2.x)



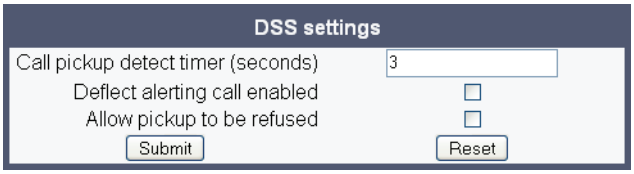
Configuration (V1R3.x upwards on OpenStage 20/40)



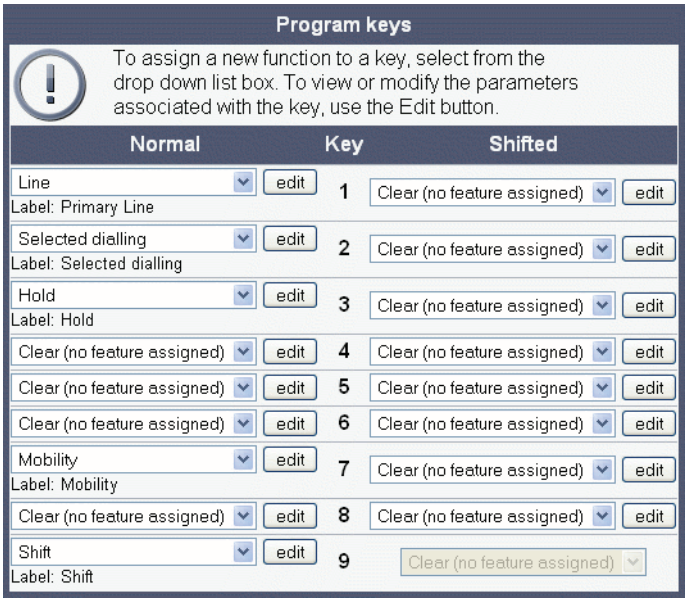
Configuration (V1R3.x upwards on OpenStage 60/80)



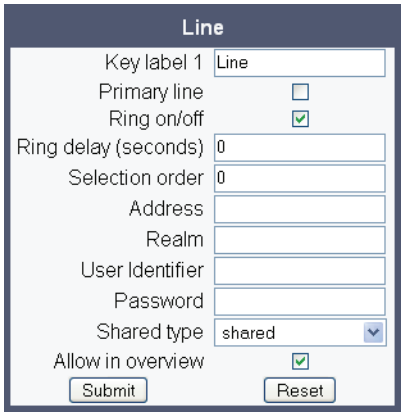
DSS settings



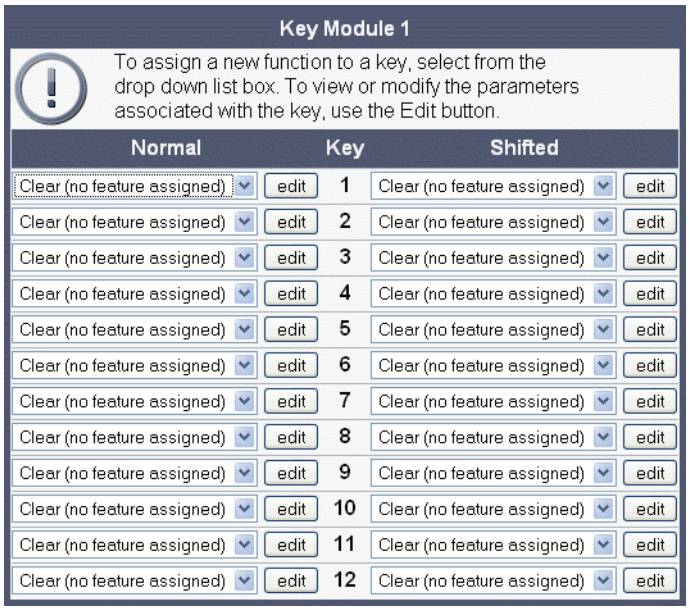
Program keys



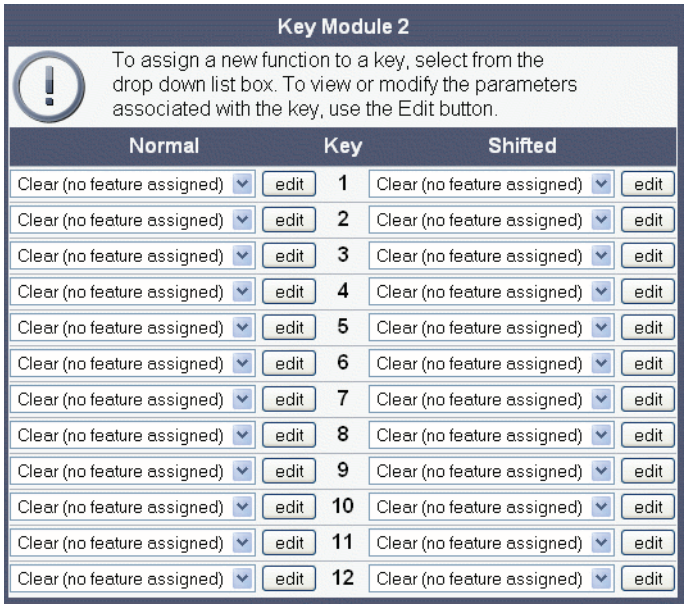
Line



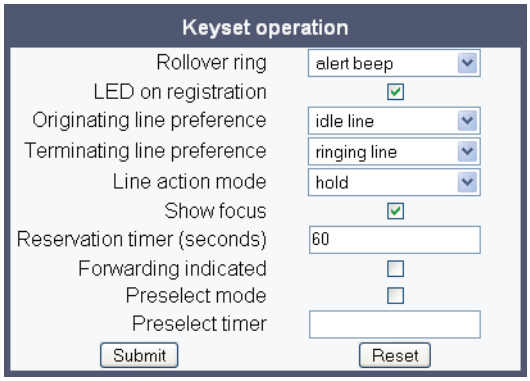
Key Module 1



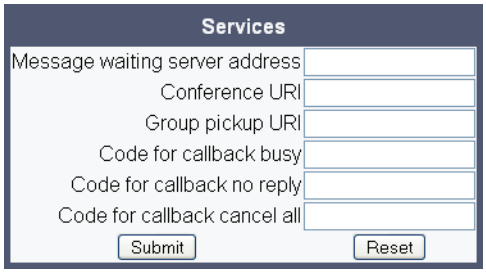
Key Module 2



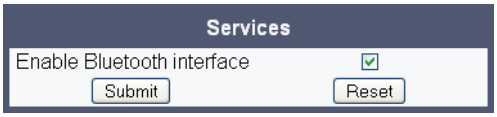
Keyset operation



Services

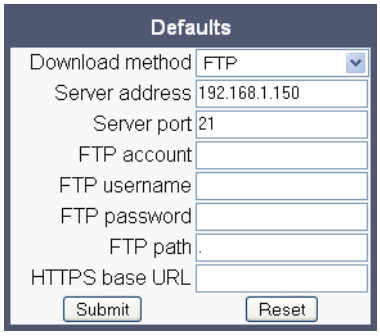


Services (V1R3.x)

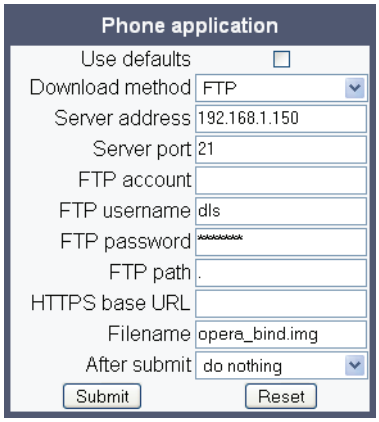


Security (V1R4.x)

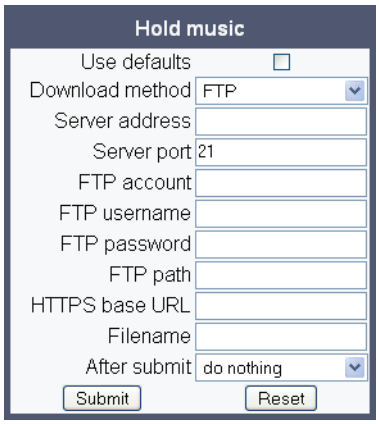
Defaults



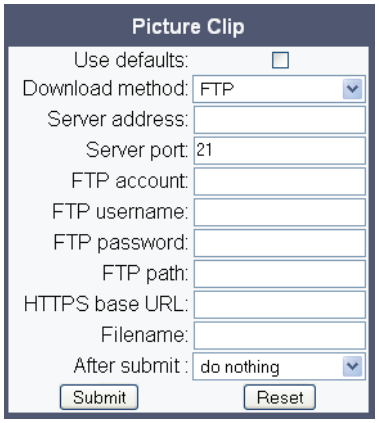
Phone application



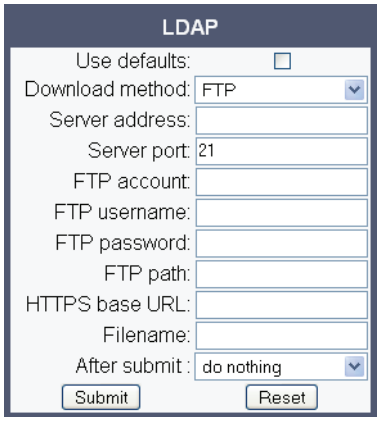
Hold music



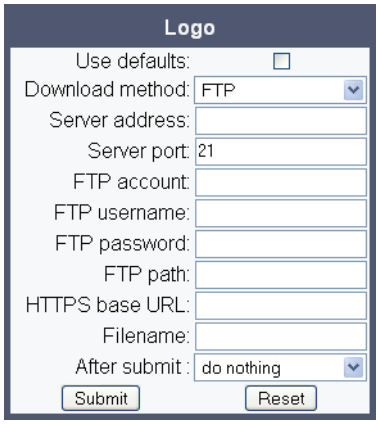
Picture Clip



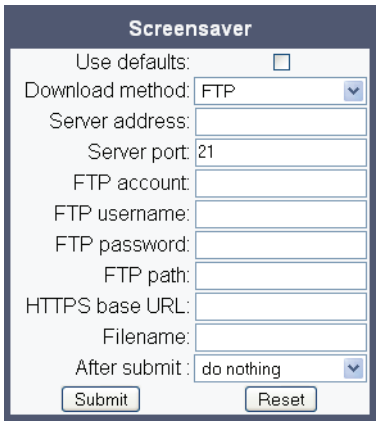
LDAP



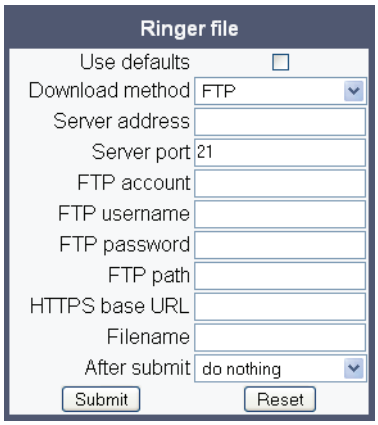
Logo



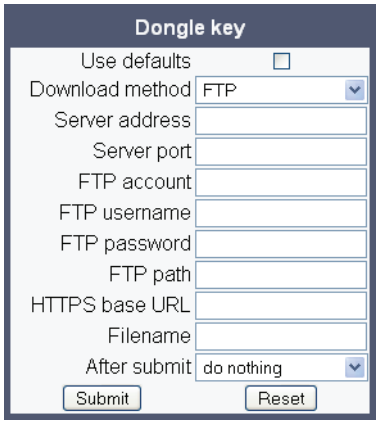
Screensaver



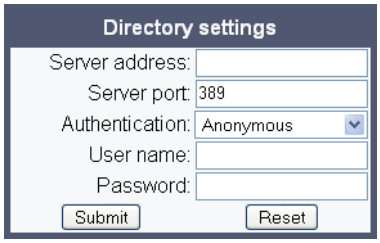
Ringer file



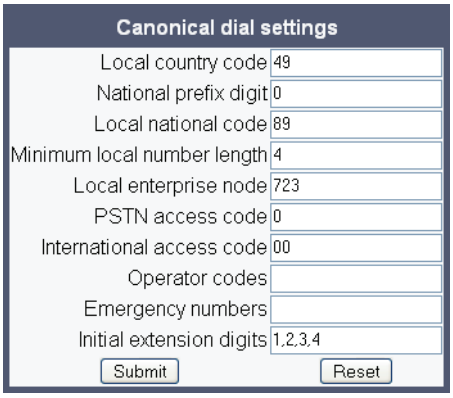
Dongle key



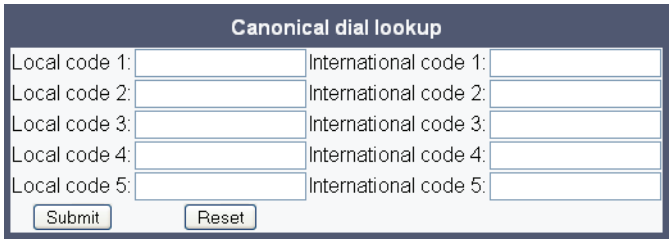
Directory settings



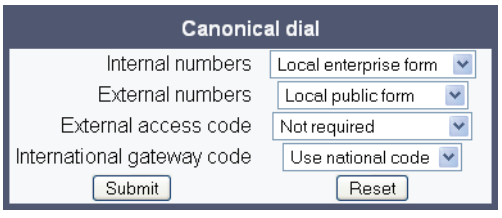
Canonical dial settings



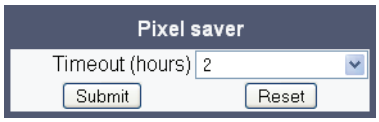
Canonical dial lookup



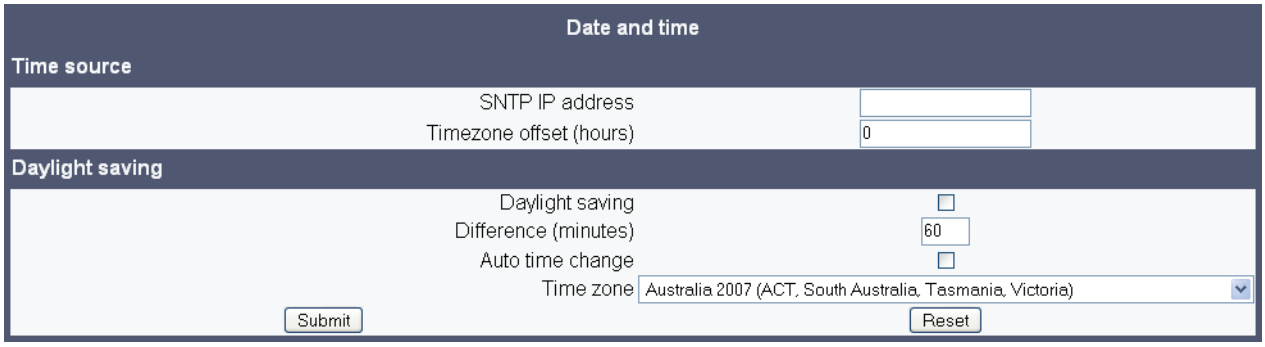
Canonical dial



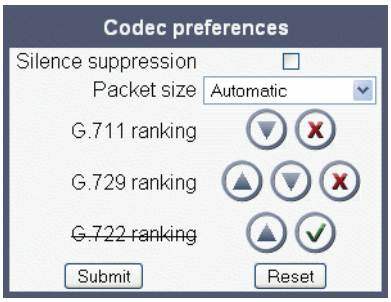
Pixel Saver (V1R4.x)



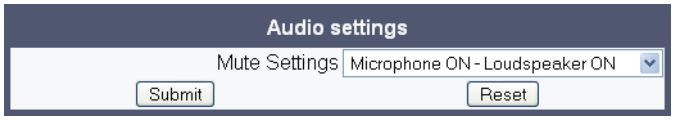
Date and time



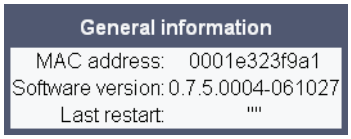
Codec preferences



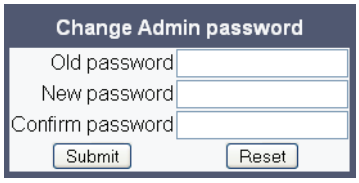
Audio settings



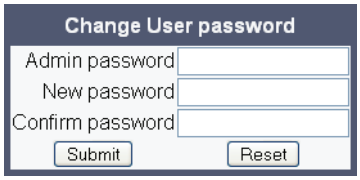
General information



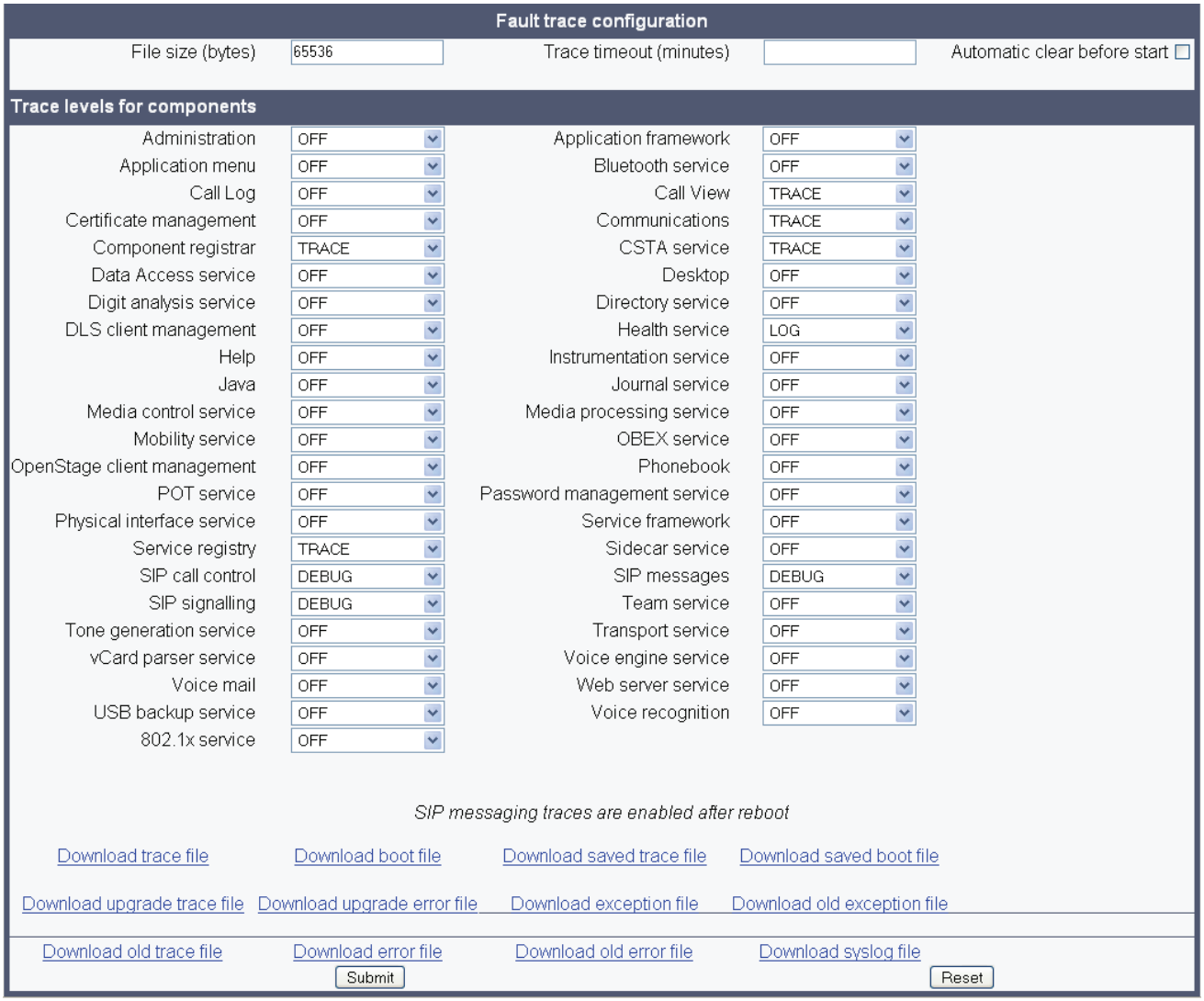
Change Admin password



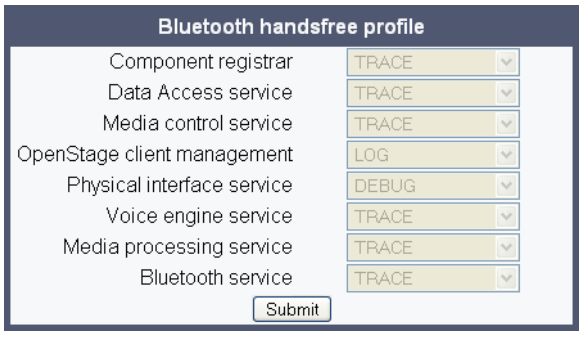
Change User password



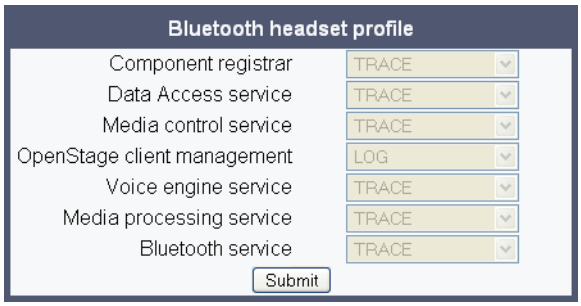
Fault trace configuration



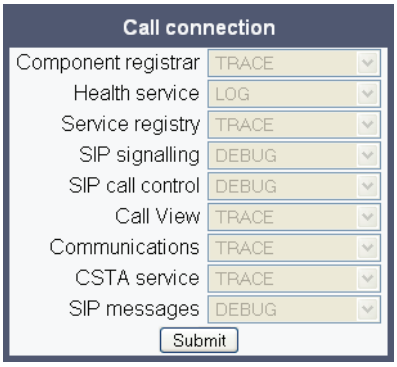
Bluetooth handsfree profile



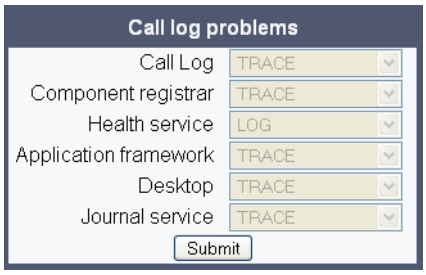
Bluetooth headset profile



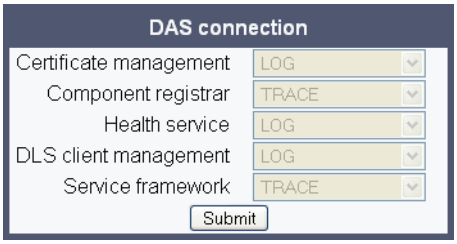
Call connection



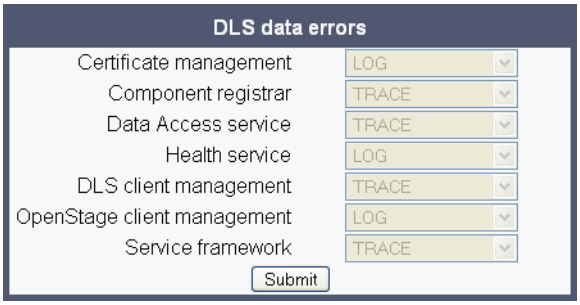
Call log problems



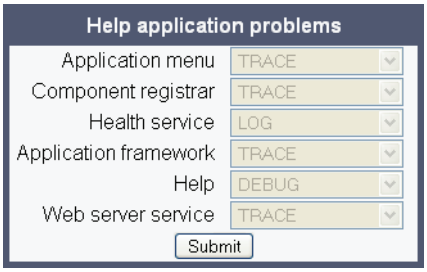
DAS connection



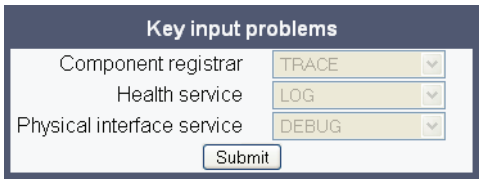
DLS data errors



Help application problems

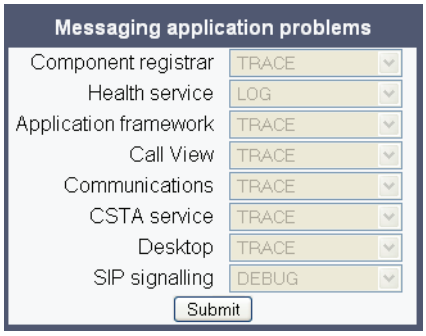


Key input problems



LAN connectivity problems

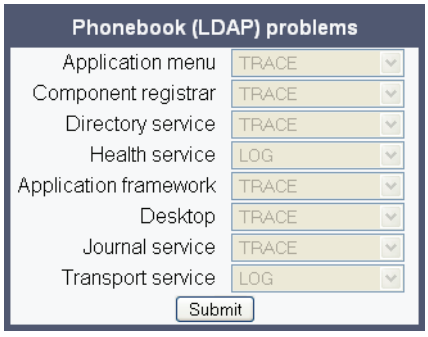
Messaging application problems



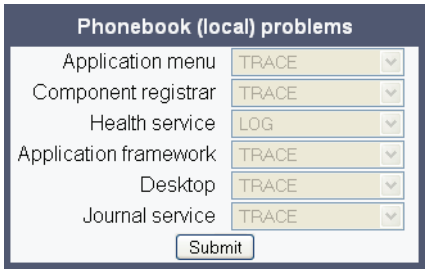
Mobility problems

Phone administration problems

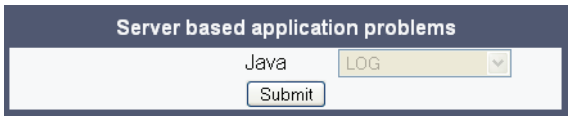
Phonebook (LDAP) problems



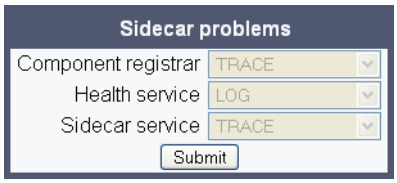
Phonebook (local) problems



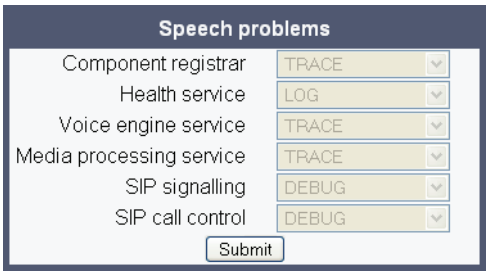
Server based application problems



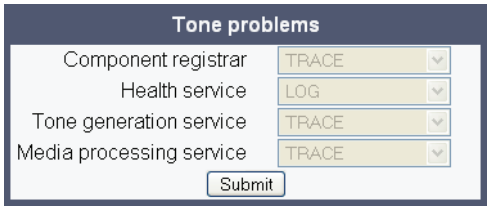
Sidecar problems



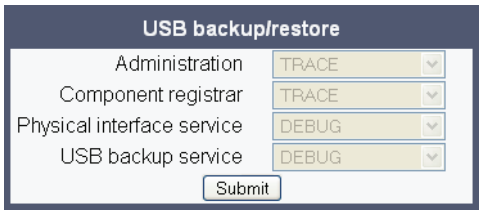
Speech problems



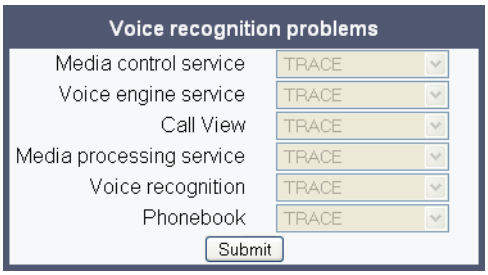
Tone problems



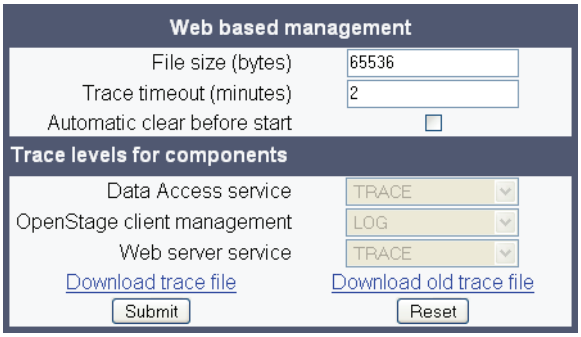
USB backup/restore



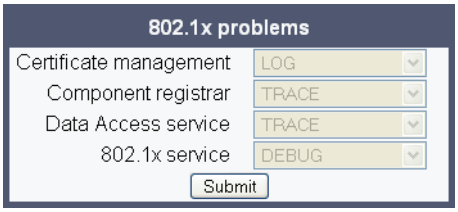
Voice recognition problems



Web based management

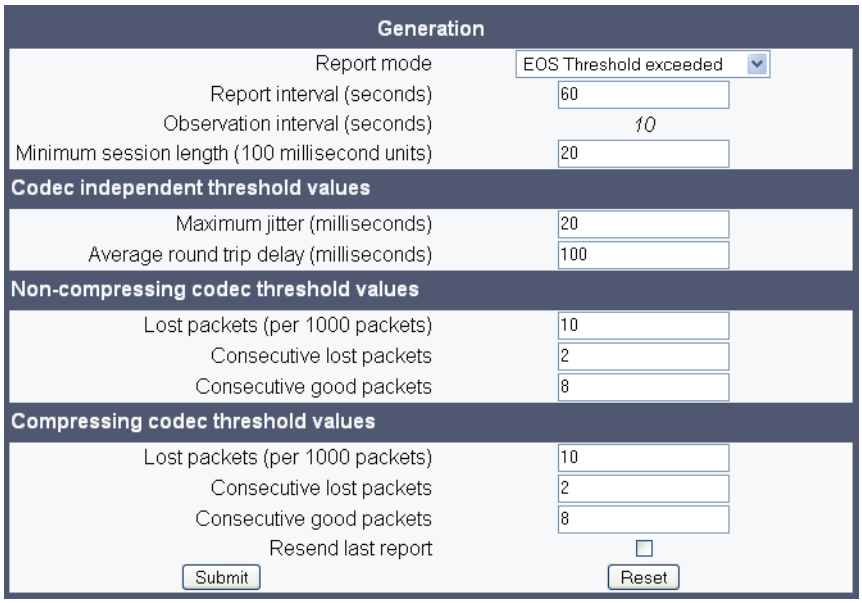


802.1x problems

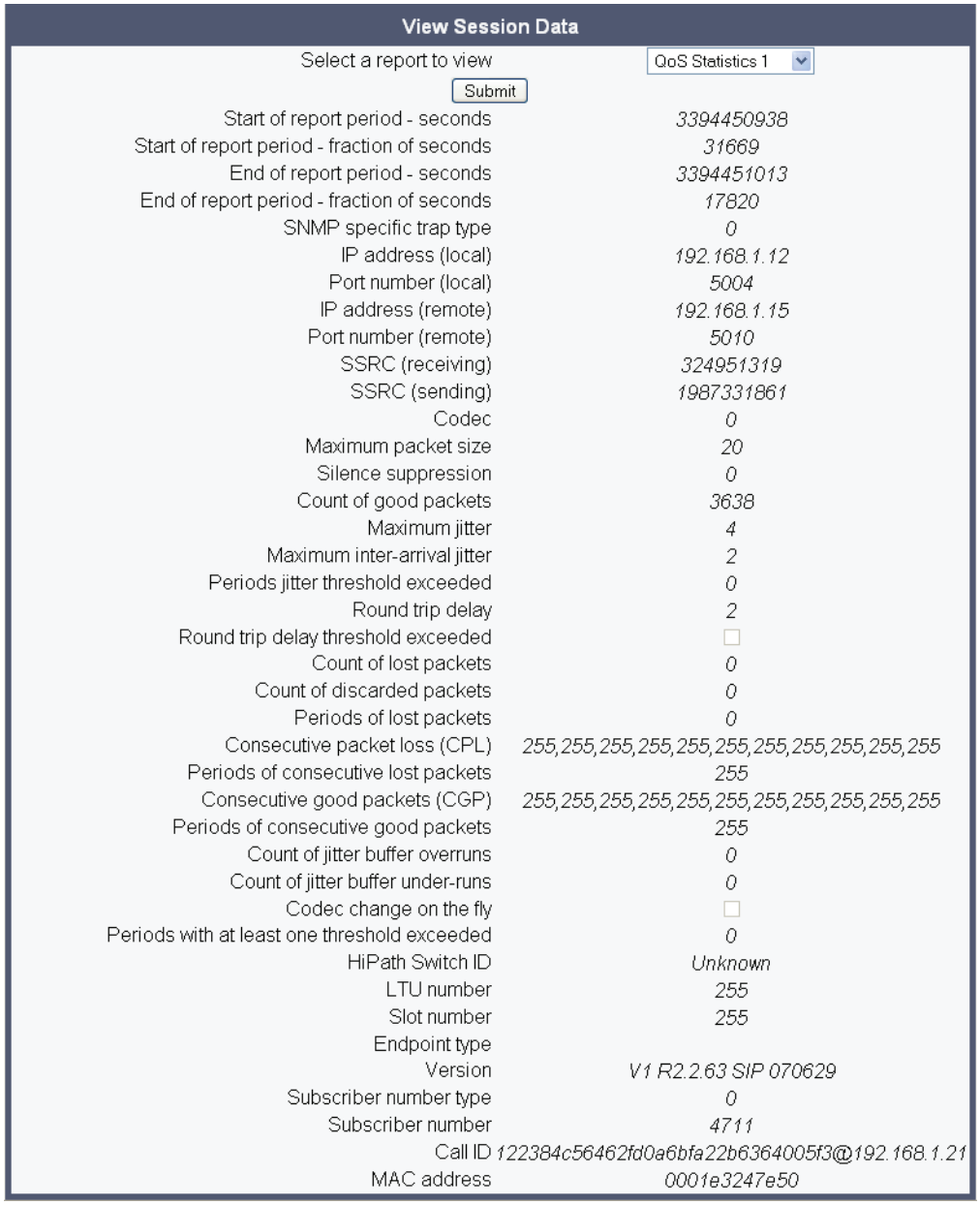


Clear all profiles

Generation

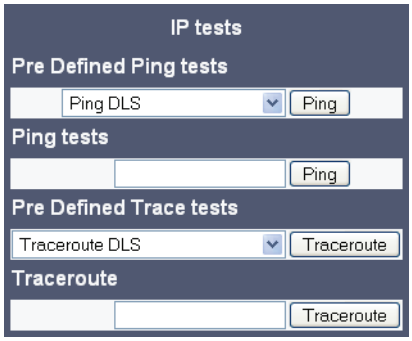

Generation
Report mode
EOS Threshold exceeded
Report interval (seconds)
60
Observation interval (seconds)
10
Minimum session length (100 millisecond units)
20
Codec independent threshold values
Maximum jitter (milliseconds)
20
Average round trip delay (milliseconds)
100
Non-compressing codec threshold values
Lost packets (per 1000 packets)
10
Consecutive lost packets
2
Consecutive good packets
8
Compressing codec threshold values
Lost packets (per 1000 packets)
10
Consecutive lost packets
2
Consecutive good packets
8
Resend last report
Submit
Reset

View Session Data

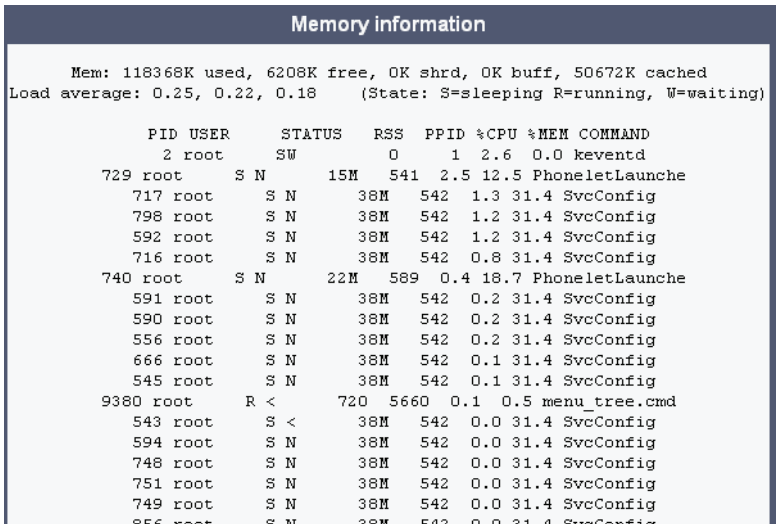


View Session Data	
Select a report to view	QoS Statistics 1
Submit	
Start of report period - seconds	3394450938
Start of report period - fraction of seconds	31669
End of report period - seconds	3394451013
End of report period - fraction of seconds	17820
SNMP specific trap type	0
IP address (local)	192.168.1.12
Port number (local)	5004
IP address (remote)	192.168.1.15
Port number (remote)	5010
SSRC (receiving)	324951319
SSRC (sending)	1987331861
Codec	0
Maximum packet size	20
Silence suppression	0
Count of good packets	3638
Maximum jitter	4
Maximum inter-arrival jitter	2
Periods jitter threshold exceeded	0
Round trip delay	2
Round trip delay threshold exceeded	
Count of lost packets	0
Count of discarded packets	0
Periods of lost packets	0
Consecutive packet loss (CPL)	255,255,255,255,255,255,255,255,255,255,255
Periods of consecutive lost packets	255
Consecutive good packets (CGP)	255,255,255,255,255,255,255,255,255,255,255
Periods of consecutive good packets	255
Count of jitter buffer overruns	0
Count of jitter buffer under-runs	0
Codec change on the fly	
Periods with at least one threshold exceeded	0
HiPath Switch ID	Unknown
LTU number	255
Slot number	255
Endpoint type	
Version	V1 R2.2.63 SIP 070629
Subscriber number type	0
Subscriber number	4711
Call ID	122384c56462fd0a6bfa22b6364005f3@192.168.1.21
MAC address	0001e3247e50

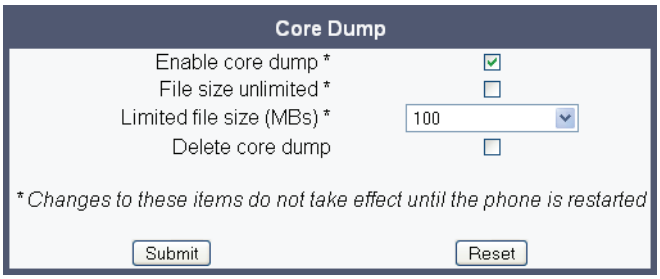
IP tests



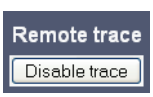
Memory information


Memory information
Mem: 118368K used, 6208K free, 0K shrd, 0K buff, 50672K cached
Load average: 0.25, 0.22, 0.18 (State: S=sleeping R=running, W=waiting)
PID USER STATUS RSS PPID %CPU %MEM COMMAND
2 root SW 0 1 2.6 0.0 keventd
729 root S N 15M 541 2.5 12.5 PhoneletLaunche
717 root S N 38M 542 1.3 31.4 SvcConfig
798 root S N 38M 542 1.2 31.4 SvcConfig
592 root S N 38M 542 1.2 31.4 SvcConfig
716 root S N 38M 542 0.8 31.4 SvcConfig
740 root S N 22M 589 0.4 18.7 PhoneletLaunche
591 root S N 38M 542 0.2 31.4 SvcConfig
590 root S N 38M 542 0.2 31.4 SvcConfig
556 root S N 38M 542 0.2 31.4 SvcConfig
666 root S N 38M 542 0.1 31.4 SvcConfig
545 root S N 38M 542 0.1 31.4 SvcConfig
9380 root R < 720 5660 0.1 0.5 menu_tree.cmd
543 root S < 38M 542 0.0 31.4 SvcConfig
594 root S N 38M 542 0.0 31.4 SvcConfig
748 root S N 38M 542 0.0 31.4 SvcConfig
751 root S N 38M 542 0.0 31.4 SvcConfig
749 root S N 38M 542 0.0 31.4 SvcConfig

Core dump



Remote trace (V1R4.x upwards)



Remote trace (V1R4.x)

Restart phone

Factory reset

HPT interface

5.1.2 Local Phone Menu

Menu	Further information ...
Administration	
Applications	
CPP	
Java	
XML	
Add application[1]	
Display name	-> Section 3.13.1
Application name	-> Section 3.13.1
Server address	-> Section 3.13.1
Server port	-> Section 3.13.1
Protocol	-> Section 3.13.1
Program name	-> Section 3.13.1
Use proxy	-> Section 3.13.1
XML trace enabled	-> Section 3.13.1
Debug program name	-> Section 3.13.1
Add Xpressions[1]	
Display name	-> Section 3.13.1
Application name	-> Section 3.13.1
Server address	-> Section 3.13.1
Server port	-> Section 3.13.1
Protocol	-> Section 3.13.1
Program name	-> Section 3.13.1
Use proxy	-> Section 3.13.1
XML trace enabled	-> Section 3.13.1
Debug program name	-> Section 3.13.1
Bluetooth	
Enable[2]	-> Section 3.18
Network	
IP configuration	
Use DHCP	-> Section 3.2.2
IP address	-> Section 3.3.3
Subnet mask	-> Section 3.3.3
Route (default)	-> Section 3.3.4
DNS domain	-> Section 3.3.6.1
Primary DNS	-> Section 3.3.6.2
Secondary DNS	-> Section 3.3.6.2
Route 1 IP	-> Section 3.3.6
Route 1 gateway	-> Section 3.3.6
Route 1 mask	-> Section 3.3.6
Route 2 IP	-> Section 3.3.6
Route 2 gateway	-> Section 3.3.6
Route 2 mask	-> Section 3.3.6
VLAN discovery	-> Section 3.2.2.1
VLAN ID	-> Section 3.2.2.2
HTTP proxy[3]	-> Section 3.13.1.2
Update Service (DLS)	
DLS address	-> Section 3.3.7

Menu	Further information ...
--- DLS port	-> Section 3.3.7
--- Contact gap	-> Section 3.3.7
--- Security status	-> Section 3.3.7
--- QoS	
--- Service	
--- Layer 2	-> Section 3.3.1.1
--- Layer 2 voice	-> Section 3.3.1.1
--- Layer 2 signalling	-> Section 3.3.1.1
--- Layer 2 default	-> Section 3.3.1.1
--- Layer 3	-> Section 3.3.1.2
--- Layer 3 voice	-> Section 3.3.1.2
--- Layer 3 signalling	-> Section 3.3.1.2
--- Reports	
--- Generation	
--- Mode	-> Section 3.17.7
--- Report interval	-> Section 3.17.7
--- Observe interval	-> Section 3.17.7
--- Minimum session length	-> Section 3.17.7
--- Send now	-> Section 3.17.7.1
--- Thresholds	
--- Maximum jitter	-> Section 3.17.7
--- Round-trip delay	-> Section 3.17.7
--- Non-compressing:	
--- ...Lost packets (K)	-> Section 3.17.7
--- ...Lost consecutive	-> Section 3.17.7
--- ...Good consecutive	-> Section 3.17.7
--- Compressing:	
--- ...Lost packets (K)	-> Section 3.17.7
--- ...Lost consecutive	-> Section 3.17.7
--- ...Good consecutive	-> Section 3.17.7
--- Port configuration	
--- SIP server	-> Section 3.5.5.2
--- SIP registrar	-> Section 3.5.5.2
--- SIP gateway	-> Section 3.5.5.2
--- SIP local	-> Section 3.5.5.2
--- Backup proxy	-> Section 3.5.9
--- RTP base	-> Section 3.12.1
--- LDAP server port	
--- LAN port type	-> Section 3.2.1
--- PC port status	-> Section 3.2.1
--- PC port type	-> Section 3.2.1
--- PC port autoMDIX	-> Section 3.2.1
--- HTTP proxy	-> Section 3.13.1.2
--- System	
--- Identity	
--- Terminal number	-> Section 3.5.1.1
--- Terminal name	-> Section 3.5.1.1
--- Display identity	-> Section 3.5.1.2
--- Enable ID	-> Section 3.5.1.2
--- SIP Interface	
--- Outbound proxy	-> Section 3.5.7.3

Menu	Further information ...
Default OBP domain	-> Section 3.5.7.3
SIP transport	-> Section 3.5.7.4
Response timer (ms)	-> Section 3.5.7.1
Connectivity timer (ms)	-> Section 3.5.7.2
Registration	
SIP addresses	
SIP server	-> Section 3.5.5.1
SIP registrar	-> Section 3.5.5.1
SIP gateway	-> Section 3.5.5.1
SIP session	
Session timer	-> Section 3.5.8
Session duration (s)	-> Section 3.5.8
Registration timer (s)	-> Section 3.5.6
Server type	-> Section 3.5.6
Realm	-> Section 3.5.6
User ID	-> Section 3.5.6
Password	-> Section 3.5.6
SIP survivability	
Backup registration flag	-> Section 3.5.9
Backup proxy address	-> Section 3.5.9
Backup registration timer (s)	-> Section 3.5.9
Backup transport	-> Section 3.5.9
OBP flag	-> Section 3.5.9
SNMP	
Trap sending enabled	-> Section 3.3.8
Trap destination	-> Section 3.3.8
Trap destination port	-> Section 3.3.8
Trap community	-> Section 3.3.8
Diagnostic sending enabled	-> Section 3.3.8
Diagnostic destination	-> Section 3.3.8
Diagnostic destination port	-> Section 3.3.8
Diagnostic community	-> Section 3.3.8
QoS traps to QCU	-> Section 3.3.8
QCU address	-> Section 3.3.8
QCU port	-> Section 3.3.8
QCU community	-> Section 3.3.8
QoS to generic destination	-> Section 3.3.8
Features	
Configuration	
General	
Emergency number	-> Section 3.5.2
Voicemail number	-> Section 3.5.2
Allow refuse	-> Section 3.6.1
Initial digit timer	-> Section 3.6.3
Allow uaCSTA	-> Section 3.6.8
Server features[4]	-> Section 3.6.7
Transfer on hangup	-> Section 3.6.3.2
Not used timeout	-> Section 3.6.9
DSS Pickup timer	-> Section 3.7.3.1
Audio	
Group pickup tone allowed[5]	-> Section 3.6.2.2

Menu	Further information ...
Group pickup as ringer[5]	-> Section 3.6.2.2
Group pickup visual alert[5]	-> Section 3.6.2.2
Keyset Lines[5]	
Details For Keyset Line <n>	
Address	-> Section 3.7.1
Ring on/off	-> Section 3.7.1
Selection order	-> Section 3.7.1
Bluetooth[1]	
Local device address	-> Section 3.18
Keyset operation[5]	
Rollover ring	-> Section 3.7.2
LED on registration	-> Section 3.7.2
Originating line preference	-> Section 3.7.2
Terminating line preference	-> Section 3.7.2
Line action mode	-> Section 3.7.2
Show focus	-> Section 3.7.2
Reservation timer	-> Section 3.7.2
Forwarding indicated	-> Section 3.7.2
Preselect mode	-> Section 3.7.2
Preselect timer	-> Section 3.7.2
Addressing	
MWI server URI	-> Section 3.6.5
Conference	-> Section 3.6.6
Group pickup URI	-> Section 3.6.2
Callback: busy	-> Section 3.6.4
Callback: no reply	-> Section 3.6.4
Callback: cancel all	-> Section 3.6.4
Feature Access	
Call establish	
Deflect to DSS	-> Section 3.7.3.1
Refuse DSS pickup	-> Section 3.7.3.1
Security[6]	
Server cerfificate	-> Section 3.4
Backup certificate	-> Section 3.4
Use secure calls	-> Section 3.4
File Transfer	
Defaults	-> Section 3.10.2
Download method	-> Section 3.10.2
Server	-> Section 3.10.2
Port	-> Section 3.10.2
Account	-> Section 3.10.2
Username	-> Section 3.10.2
Password	-> Section 3.10.2
FTP path	-> Section 3.10.2
HTTPS base URL	-> Section 3.10.2
Phone app	-> Section 3.10.3
Use default	-> Section 3.10.3.1
Download method	-> Section 3.10.3.1
Server	-> Section 3.10.3.1
Port	-> Section 3.10.3.1
Account	-> Section 3.10.3.1

Menu	Further information ...
Username	-> Section 3.10.3.1
Password	-> Section 3.10.3.1
FTP path	-> Section 3.10.3.1
HTTPS base URL	-> Section 3.10.3.1
Filename	-> Section 3.10.3.1
Hold Music	
Use default	-> Section 3.10.4.1
Download method	-> Section 3.10.4.1
Server	-> Section 3.10.4.1
Port	-> Section 3.10.4.1
Account	-> Section 3.10.4.1
Username	-> Section 3.10.4.1
Password	-> Section 3.10.4.1
FTP path	-> Section 3.10.4.1
HTTPS base URL	-> Section 3.10.4.1
Filename	-> Section 3.10.4.1
Ringer	
Use default	-> Section 3.10.6.1
Download method	-> Section 3.10.6.1
Server	-> Section 3.10.6.1
Port	-> Section 3.10.6.1
Account	-> Section 3.10.6.1
Username	-> Section 3.10.6.1
Password	-> Section 3.10.6.1
FTP path	-> Section 3.10.6.1
HTTPS base URL	-> Section 3.10.6.1
Filename	-> Section 3.10.6.1
Picture clip[3]	
Use default	-> Section 3.10.5.1
Download method	-> Section 3.10.5.1
Server	-> Section 3.10.5.1
Port	-> Section 3.10.5.1
Account	-> Section 3.10.5.1
Username	-> Section 3.10.5.1
Password	-> Section 3.10.5.1
FTP path	-> Section 3.10.5.1
HTTPS base URL	-> Section 3.10.5.1
Filename	-> Section 3.10.5.1
LDAP[3]	
Use default	-> Section 3.10.6.1
Download method	-> Section 3.10.6.1
Server	-> Section 3.10.6.1
Port	-> Section 3.10.6.1
Account	-> Section 3.10.6.1
Username	-> Section 3.10.6.1
Password	-> Section 3.10.6.1
FTP path	-> Section 3.10.6.1
HTTPS base URL	-> Section 3.10.6.1
Filename	-> Section 3.10.6.1
Logo[5]	
Use default	-> Section 3.10.7.1

Menu	Further information ...
--- Download method	-> Section 3.10.7.1
--- Server	-> Section 3.10.7.1
--- Port	-> Section 3.10.7.1
--- Account	-> Section 3.10.7.1
--- Username	-> Section 3.10.7.1
--- Password	-> Section 3.10.7.1
--- FTP path	-> Section 3.10.7.1
--- HTTPS base URL	-> Section 3.10.7.1
--- Filename	-> Section 3.10.7.1
--- Screensaver[3]	
--- Use default	-> Section 3.10.8.1
--- Download method	-> Section 3.10.8.1
--- Server	-> Section 3.10.8.1
--- Port	-> Section 3.10.8.1
--- Account	-> Section 3.10.8.1
--- Username	-> Section 3.10.8.1
--- Password	-> Section 3.10.8.1
--- FTP path	-> Section 3.10.8.1
--- HTTPS base URL	-> Section 3.10.8.1
--- Filename	-> Section 3.10.8.1
--- Java midlets[7]	
--- Use default	
--- Download method	
--- Server	
--- Port	
--- Account	
--- Username	
--- Password	
--- FTP path	
--- HTTPS base URL	
--- Filename	
--- HPT dongle	
--- Use default	
--- Download method	
--- Server	
--- Port	
--- Account	
--- Username	
--- Password	
--- FTP path	
--- HTTPS base URL	
--- Filename	
--- Local Functions	
--- Directory Settings[3]	
--- LDAP server address	-> Section 3.11.1
--- LDAP server port	-> Section 3.11.1
--- LDAP authenticate	-> Section 3.11.1
--- LDAP user name	-> Section 3.11.1
--- LDAP password	-> Section 3.11.1
--- Locality	
--- Canonical settings	

Menu	Further information ...
--- Local country code	-> Section 3.8.1
--- National prefix digit	-> Section 3.8.1
--- Local national code	-> Section 3.8.1
--- Minimum local number length	-> Section 3.8.1
--- Local enterprise node	-> Section 3.8.1
--- PSTN access code	-> Section 3.8.1
--- International access code	-> Section 3.8.1
--- Operator code	-> Section 3.8.1
--- Emergency number	-> Section 3.8.1
--- Initial digits	-> Section 3.8.1
--- Canonical lookup	
--- Local code 1	-> Section 3.8.2
--- International code 1	-> Section 3.8.2
--- Local code 2	-> Section 3.8.2
--- International code 2	-> Section 3.8.2
--- Local code 3	-> Section 3.8.2
--- International code 3	-> Section 3.8.2
--- Local code 4	-> Section 3.8.2
--- International code 4	-> Section 3.8.2
--- Local code 5	-> Section 3.8.2
--- International code 5	-> Section 3.8.2
--- Canonical dial	
--- Internal numbers	-> Section 3.8.1
--- External numbers	-> Section 3.8.1
--- External access code	-> Section 3.8.1
--- International gateway	-> Section 3.8.1
--- Pixel saver	-> Section 3.5.3
--- Date and Time	
--- Time source	-> Section 3.5.4.1
--- SNTP IP address	-> Section 3.5.4.1
--- Timezone offset	-> Section 3.5.4.1
--- Daylight saving	-> Section 3.5.4.1
--- Daylight saving	-> Section 3.5.4.1
--- Difference (mins)	-> Section 3.5.4.1
--- Auto DST	-> Section 3.5.4.1
--- DST zone	-> Section 3.5.4.1
--- Speech	
--- Codec Preferences	
--- Silence suppression	-> Section 3.12.2
--- Packet size	-> Section 3.12.2
--- G.711	-> Section 3.12.2
--- G.729	-> Section 3.12.2
--- G.722	-> Section 3.12.2
--- Audio Settings	
--- Disable microphone	-> Section 3.12.3
--- Disable loudspeech	-> Section 3.12.3
--- General Information	
--- MAC address	-> Section 3.17.1
--- Software version	-> Section 3.17.1
--- Last restart	-> Section 3.17.1
--- Password	

Menu	Further information ...
Admin	-> Section 3.14
Confirm admin	-> Section 3.14
User	-> Section 3.14
Confirm user	-> Section 3.14
Mobility	
Unauthorized logoff trap	-> Section 3.9
Logoff trap delay	-> Section 3.9
Timer med priority	-> Section 3.9
Mobility feature	-> Section 3.9
Managed profile	
Error count local	
Error count remote	
Maintenance	
Factory reset	-> Section 3.16
Disable HPT	-> Section 3.17.10
Remote trace[4]	
Remote trace status	-> Section 3.17.9
Remote ip	-> Section 3.17.9
Remote port	-> Section 3.17.9

1 OpenStage 60/80 V1R3.x upwards only.
2 OpenStage 60/80 V1R2.x only. In V1R3.x, Bluetooth can be enabled or disabled only via WBM or DLS.
3 OpenStage 60/80 only.
4 V1R3.x upwards only.
5 OpenStage 40/60/80 only.
6 V1R4.x upwards.
7 Not available yet.

Glossary

A

Address of Record (AoR)
A ->SIP ->URI that represents the "public address" of a SIP user resp. a phone or line. The format is similar to an E-mail address: "username@hostname". (for a definition, see RFC 3261)

ADPCM
Adaptive **D**ifferential **P**ulse **C**ode **M**odulation. A compressed encoding method for audio signals which are to be transmitted by a low bandwidth. As opposed to regular ->PCM, a sample is coded as the difference between its predicted value and its real value. As this difference is usually smaller than the real, absolute value itself, a lesser number of bits can be used to encode it.

C

CSTA
Computer **S**upported **T**elecommunications **A**pplications. An abstraction layer for telecommunications applications allowing for the interaction of ->CTI computer applications with telephony devices and networks.

CTI
Computer **T**elephony **I**ntegration. This term denotes the interaction of computer applications with telephony devices and networks.

D

DFT
Digital **F**eature **T**elephone. A phone with no line keys.

DHCP
Dynamic **H**ost **C**onfiguration **P**rotocol. Allows for the automatic configuration of network endpoints, like IP Phones and IP Clients.

DiffServ
Differentiated **Serv**ices. Specifies a layer 3 mechanism for classifying and managing network traffic and providing quality of service (->QoS) guarantees on ->IP networks. DiffServ can be used to provide low-latency, guaranteed service for e. g. voice or video communication.

DLS
The Deployment Service (DLS) is a HiPath management application for the administration of workpoints, i. e. IP Phones and IP Clients, in both HiPath- and non-HiPath networks.

DNS
Domain **N**ame **S**ystem. Performs the translation of network domain names and computer hostnames to ->IP addresses.

DTMF
Dual **T**one **M**ulti **F**requency. A means of signaling between a phone and e. g. a voicemail facility. The signals can be transmitted either in-band, i. e. within the speech band, or out-band, i. e. in a separate signaling channel.

E

EAP
Extensible **A**uthentication **P**rotocol. An authentication framework that is frequently used in WLAN networks. It is defined in RFC 3748.

F

FTP
File **T**ransfer **P**rotocol. Used for transferring files in networks, e. g., to update telephone software.

G

G.711
ITU-T standard for audio encoding, used in ISDN and ->VoIP. It requires a 64 kBit/s bandwidth.

G.722
ITU-T standard for audio encoding using split band ->ADPCM. The audio bandwidth is 7 kHz at a sampling rate of 16 kHz. There are several transfer rates ranging from 32 to 64 kBit/s, which correspond to different compression degrees. The voice quality is very good.

G.729
ITU-T standard for audio encoding with low bandwidth requirements, mostly used in VoIP. The standard bitrate is 8 kBit/s. Music or tones such as ->DTMF or fax tones cannot be transported reliably with this codec.

Gateway
Mediation components between two different network types, e. g., ->IP network and ISDN network.

GUI
Graphical **U**ser **I**nterface.

H

HTTP
Hyper**t**ext **T**ransfer **P**rotocol. A standard protocol for data transfer in ->IP networks.

I

IP
Internet **P**rotocol. A data-oriented network layer protocol used for transferring data across a packet-switched internetwork. Within this network layer, reliability is not guaranteed.

IP address
The unique address of a terminal device in the network. It consists of four number blocks of 0 to 255 each, separated by a point.

J

Jitter
Latency fluctuations in the data transmission resulting in distorted sound.

L

LAN
Local **A**rea **N**etwork. A computer network covering a local area, like an office, or group of buildings.

Layer 2
2nd layer (Data Link Layer) of the 7-layer OSI model for describing data transmission interfaces.

Layer 3
3rd layer (Network Layer) of the 7-layer OSI model for describing the data transmission interfaces.

LCD
Liquid **C**rystal **D**isplay. Display of numbers, text or graphics with the help of liquid crystal technology.

LDAP
Lightweight **D**irectory **A**ccess **P**rotocol. Simplified protocol for accessing standardized directory systems, e.g., a company telephone directory.

LED
Light **E**mitting **D**iode. Cold light illumination in different colours at low power consumption.

M

MAC Address
Media **A**ccess **C**ontrol address. Unique 48-bit identifier attached to network adapters.

MDI-X
Media **D**ependent **I**nterface crossover (**X**). The send and receive pins are inverted. This MDI allows the connection of two endpoints without using a crossover cable. When Auto MDI-X is available, the MDI can switch between regular MDI and MDI-X automatically, depending on the connected device.

MIB
Management **I**nformation **B**ase. A type of database used to manage the devices in a communications network.

MWI
Message **W**aiting **I**ndicator. A signal, typically a LED, to notify the user that new mailbox messages have arrived.

P

PBX
Private **B**ranch E**x**change. Private telephone system that connects the internal devices to each other and to the ISDN network.

PCM
Pulse **C**ode **M**odulation. A digital representation of an analog signal, e. g. audio data, which consists of quantized samples taken in regular time intervals.

PING
Packet **In**ternet **G**ro(u)per. A program to test whether a connection can be made to a defined IP target. Data is sent to the target and returned from there during the test.

PoE
Power **o**ver **E**thernet. The IEEE 802.3af standard specifies how to supply power to compliant devices over Ethernet cabling (10/100Base-T).

Port
Ports are used in ->IP networks to permit several communication connections simultaneously. Different services often have different port numbers.

PSTN
Public **S**witched **T**elephone **N**etwork. The network of the world's public circuit-switched telephone networks.

Q

QoS

Quality **o**f **S**ervice. The term refers to control mechanisms that can provide different priority to different users or data flows, or guarantee a certain level of performance to a data flow in accordance with requests from the application program. The OpenStage phone allows for the setting of QoS parameters on layer 2 and layer 3 (DiffServ).

QDC

QoS **D**ata **C**ollection. A HiPath IP service that is used to collect data from HiPath products in order to analyze their voice and network quality.

QCU

Quality of Service Data **C**ollection **U**nit. A service tool that collects QoS report data from IP endpoints.

QoS

Quality **o**f **S**ervice. Provides different priority to different users or data flows, or guarantee a certain level of performance to a data flow.

R

RAM

Random **A**ccess **M**emory. Memory with read / write access.

ROM

Read **O**nly **M**emory. Memory with read only access.

RTCP

Realtime **T**ransport **C**ontrol **P**rotocol. Controls the ->RTP stream and provides information about the status of the transmission, like QoS parameters.

RTP

Realtime **T**ransport **P**rotocol. This application layer protocol has been designed for audio and video communication. Typically, the underlying protocol is ->UDP.

S

SDP

Session **D**escription **P**rotocol. Describes and initiates multimedia sessions, like web conferences. The informations provided by SDP can be processed by ->SIP.

SIP

Session **I**nitiation **P**rotocol. Signaling protocol for initialising and controlling sessions, used e. g. for ->VoIP calls.

SNMP
Simple **N**etwork **M**anagement **P**rotocol. Used for monitoring, controlling, and administration of network and network devices.

SNTP
Simple **N**etwork **T**ime **P**rotocol. Used to synchronize the time of a terminal device with a timeserver.

Subnet Mask
To discern the network part from the host part of an ->IP address, a device performs an AND operation on the IP address and the network mask. The network classes A, B, and C each have a subnet mask that demasks the relevant bits: 255.0.0.0 for Class A, 255.255.0.0 for Class B and 255.255.255.0 for Class C. In a Class C network, for instance, 254 IP addresses are available.

Switch
Network device that connects multiple network segments and terminal devices. The forwarding of data packets is based on ->MAC Addresses: data targeted to a specific device is directed to the switch port that device is attached to.

T

TCP
Transfer **C**ontrol **P**rotocol. The protocol belongs to the transport layer and establishes a connection between two entities on the application layer. It guarantees reliable and in-order delivery of data from sender to receiver, as opposed to ->UDP.

TLS
Transport **L**ayer **S**ecurity. Ensures privacy between communicating applications. Typically, the server is authenticated, but mutual authentication is also possible.

U

UDP
User **D**atagram **P**rotocol. A minimal message-oriented transport layer protocol used especially in streaming media applications such as ->VoIP. Reliability and order of packet delivery are not guaranteed, as opposed to ->TCP, but ->UDP is faster and more efficient.

URI
Uniform **R**esource **I**dentifier. A compact string of characters used to identify or name a resource.

URL
Uniform **R**esource **L**ocator. A special type of ->URI which provides means of acting upon or obtaining a representation of the resource by describing its primary access mechanism or network location.

V

VLAN

Virtual **L**ocal **A**rea **N**etwork. A method of creating several independent logical networks within a physical network. For example, an existing network can be separated into a data and a voice VLAN.

VoIP

Voice **o**ver **IP**. A term for the protocols and technologies enabling the routing of voice conversations over the internet or through any other ->IP-based network

W

WAP

Wireless **A**pplication **P**rotocol. A collection of protocols and technologies aiming at enabling access to internet applications for wireless devices. WAP can also be used by the OpenStage phone.

WBM

Web **B**ased **M**anagement. A web interface which enables configuration of the device using a standard web browser.

WML

Wireless **M**arkup **L**anguage. An XML-based markup language which supports text, graphics, hyperlinks and forms on a ->WAP-browser.

WSP

Wireless **S**ession **P**rotocol. The protocol is a part of the ->WAP specification. Its task is to establish a session between the terminal device and the WAP gateway.

Index

A

Address of Record (AoR) 6-1
Administration Menu (Local Menu) 3-1, 3-2
Application Keys 1-4, 1-6
Audio Keys 1-4, 1-5

B

Bluetooth 3-149

C

Call Display 1-4, 1-5
Call Transfer 3-50
Callback 3-52
Canonical Dial Lookup 3-76
Canonical Dialing 3-72
Conference (System based) 3-54
CSTA 3-56, 6-1
CTI 6-1

D

Date and Time (SNTP) 2-10, 3-30
Daylight Saving 3-30
Default Route 3-16
DFT (Digital Feature Telephone) 6-1
DHCP 3-13, 6-1
Diffserv 3-11
DLS (Deployment Service) 1-7, 3-20, 6-2
DNS 3-18, 6-2
DNS Domain Name 3-18
DST Zone (Daylight Saving Time Zone) 3-30

E

Emergency Number 3-27, 3-72
External Access Code 3-73
External Numbers 3-73

F

FTP Settings 3-79
Function Keys 1-4, 1-5, 1-6

G

Graphics Display 1-4
Group Pickup 3-47

H

Handset 1-4, 1-6
HiPath 8000 (Registration) 2-25

I

Initial Digits 3-73
Internal Numbers 3-73
International Code (Local Country Code) 3-72
International Gateway Code 3-74
International Prefix (International Access Code) 3-72
IP
- Address 2-10
- Address (Manual Configuration) 3-15
- IP 6-3
- Specific Routing 3-17

K

Keypad 1-4, 1-5, 1-6

L

LAN 6-3
LAN Port 3-5
LDAP 6-3
LDAP Template (Download) 3-91
Line Key Configuration 3-60
Local Area Code (Local National Code) 3-72
Local Country Code (International Code) 3-72
Local Enterprise Number 3-72
Local National Code (Local Area Code) 3-72
Logo (Create) 4-5
Logo (Download) 3-94

M

MAC Address 6-4

MDI-X 3-5, 6-4
MIB 6-4
Multiline / Keyset 3-60
Music on Hold (Download) 3-84
MWI 3-53
MWI (Message Waiting Indicator) 6-4

N

National Prefix (Trunk Prefix) 3-72

O

Operator Code 3-72
Outbound Proxy 3-38

P

Password, change 3-118
Password, enter 3-1
PBX 6-4
Phone Software (Download) 3-81
Picture Clips (Download) 3-88
PoE (Power over Ethernet) 2-5, 6-4
Program Keys 1-4, 1-5
PSTN 6-4
PSTN Aaccess Code 3-72

Q

QCU 3-22
QoS 3-10

R

RTP 6-5

S

Screensaver (Download) 3-97
SIP
- Registration 3-35
- Server Addresses 3-33
- Server Ports 3-34
- Session Timer 3-40
- Transport Protocol 3-39

SNMP 3-21, 6-6
Subnet Mask 2-10
Subnet Mask (Manual Configuration) 3-15
Survivability 3-42

T

TCP 6-6
Terminal Number 2-8, 3-25
Timeout (Not used) 3-58
Timezone Offset 2-10, 3-30
TLS 6-6
TouchGuide 1-4, 1-6
TouchSlider 1-4
Trunk Prefix (National Prefix) 3-72

U

uaCSTA 3-56
UDP 6-6

V

Vendor Class (DHCP) 2-12
VLAN 2-11, 3-7
Voice Mail Number 3-27

W

WBM (Web Based Management) 1-6, 2-7, 6-7

Communication for the open minded

Siemens Enterprise Communications
www.siemens.com/open

Copyright © Siemens Enterprise Communications GmbH & Co. KG 13/06/2008
Hofmannstr. 51, D-81359 München

Reference No.: A31003-O1010-M100-10-76A9

The information provided in this document contains merely general descriptions or characteristics of performance which in case of actual use do not always apply as described or which may change as a result of further development of the products. An obligation to provide the respective characteristics shall only exist if expressly agreed in the terms of contract. Subject to availability. Right of modification reserved. The trademarks used are owned by Siemens Enterprise Communications GmbH & Co. KG or their respective owners.